

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-305662

(43)公開日 平成8年(1996)11月22日

(51)Int.Cl. <sup>6</sup>	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0	9364-5L	G 0 6 F 15/00	3 3 0 C
13/00	3 5 1	7368-5E	13/00	3 5 1 E

審査請求 未請求 請求項の数9 O L (全 22 頁)

(21)出願番号 特願平7-108408

(22)出願日 平成7年(1995)5月2日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72)発明者 秋山 良太

神奈川県川崎市中原区上小田中1015番地  
富士通株式会社内

(72)発明者 宗像 昭夫

神奈川県川崎市中原区上小田中1015番地  
富士通株式会社内

(74)代理人 弁理士 遠山 勉 (外1名)

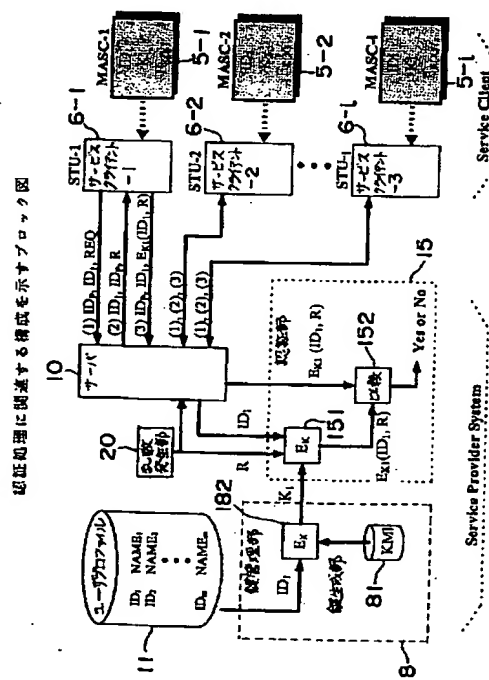
最終頁に続く

(54)【発明の名称】 クライアント認証システムおよび方法

(57)【要約】

【目的】クライアントとサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方において動的に作成することにより、これらの第三者による盗用が不可能となるクライアント認証システムを提供する。

【構成】サービス提供者側システム1の鍵管理部18は、アクセス要求を行ったサービスクライアント6に接続されたMASC5に対応する個別鍵Kを生成し、この個別鍵Kを認証部15に通知する。この個別鍵は、予め、MASC5にも格納されている。乱数発生器20は、乱数Rを生成して、MASC5に送信するとともに、認証部15に通知する。MASC5は、この乱数を個別鍵によって暗号化して、サービス提供者側システム1に戻す。一方、認証部15の暗号化部151は、乱数Rを個別鍵Kによって暗号化する。そして、認証部15の比較器152は、暗号化部151が暗号化したデータとMASC5から送信されてきた暗号化データを比較して、両者が一致した場合には、このMASC5からのアクセス要求であると確認する。



## 【特許請求の範囲】

【請求項1】データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して配送されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証システムにおいて、前記データ供給装置は、前記クライアントに対応する第1の鍵を出力する鍵出力部と、前記クライアントからのアクセス要求に応じて乱数を発生する乱数発生手段と、前記鍵出力部において出力された第1の鍵によって前記乱数を暗号化することによって第1の認証子を出力する第1の暗号化手段と、前記クライアントに前記乱数を送信する第1の送信手段と、前記クライアントから第2の認証子を受信する第1の受信手段と、前記第1の認証子と前記第2の認証子とを比較して両者が一致している場合に当該クライアントからのアクセス要求であると認証する比較手段とを備え、前記クライアントは、前記データ供給装置にアクセス要求を行うアクセス要求手段と、前記データ供給装置から送信された前記乱数を受信する第2の受信手段と、前記第1の鍵と同一の第2の鍵を保持する鍵保持手段と、前記第2の鍵によって前記乱数を暗号化することによって前記第2の認証子を出力する第2の暗号化手段と、前記データ供給装置に前記第2の認証子を送信する第2の送信手段とを備えることを特徴とするクライアント認証システム。

【請求項2】前記アクセス要求手段は、前記アクセス要求に際してそのクライアントに設定された固有の識別情報を前記データ供給装置に通知するとともに、前記鍵出力部は、各クライアントに固有の前記識別情報を加工することにより前記第1の鍵を生成することを特徴とする請求項1記載のクライアント認証システム。

【請求項3】前記データ供給装置は前記比較手段によって前記両認証子が一致すると判断された場合のみ前記データを前記クライアントに配送することを特徴とする請求項1記載のクライアント認証システム。

【請求項4】前記データ供給装置は暗号化された前記データを前記クライアントに配送するとともに、前記クライアントは前記暗号化された前記データを復号化する第1の復号化手段を備えることを特徴とする請求項1記載のクライアント認証システム。

【請求項5】前記データ供給装置は前記データを復号化するための第3の鍵を前記第1の鍵によって暗号化する第3の暗号化手段を備えているとともに、

前記クライアントは前記暗号化された前記第3の鍵を前記第2の鍵によって復号化する第2の復号化手段を備え、前記第1の復号化手段はこの第2の復号化手段によって復号化された前記第3の鍵によって前記暗号化されたデータを復元することを特徴とする請求項4記載のクライアント認証システム。

【請求項6】前記データ供給装置は、前記暗号化されたデータを格納するための複数の格納装置を備えるとともに、一方の格納装置に格納されている前記暗号化されたデータを前記第3の鍵を用いて復号化する第3の復号化手段と、第3の鍵を更新する鍵更新手段と、第3の復号化手段によって復号化されたデータを前記鍵更新手段によって更新された前記第3の鍵によって暗号化する第3の暗号化手段と、第3の暗号化手段によって暗号化されたデータを他の前記格納装置に格納する書込手段とを更に備えたことを特徴とする請求項5記載のクライアント認証システム。

【請求項7】前記第3の復号化手段、前記鍵更新手段、前記第3の暗号化手段、及び前記書込手段は一定時間毎に起動することを特徴とする請求項6記載のクライアント認証システム。

【請求項8】前記クライアントは、前記データを受信する本体部とこの本体部に対して着脱自在に設けられたモジュール部とから構成されるとともに、少なくとも前記鍵保持手段及び前記第2の暗号化手段は前記モジュール部に備えられていることを特徴とする請求項1記載のクライアント認証システム。

【請求項9】データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して送出されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証方法において、前記クライアントは自己を識別する識別情報を付して前記データ供給装置にアクセス要求を行い、前記データ供給装置は、このアクセス要求に応じて乱数を発生してこの乱数を前記クライアントに送出するとともに、前記識別情報に対応する第1の鍵によって前記乱数を暗号化して第1の認証子に変換し、前記クライアントは前記第1の鍵と同一内容を有するものとして予め保持している第2の鍵によって前記乱数を暗号化して第2の認証子に変換するとともに、この第2の認証子を前記データ供給装置に送出し、前記データ供給装置は前記第1の認証子と前記第2の認証子とを比較して両者が一致した場合に前記クライアントからのアクセス要求があったことを認証することを特徴とするクライアント認証方法。

## 【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、クライアントからの要求に応じて、映像著作物等のソフトウェアを通信手段を介して配送するシステム（デジタル・オーディオ・インタラクティブ・システム）におけるクライアント認証システム及び認証方法に関する。

#### 【0002】

【従来の技術】近年、ケーブルテレビジョンシステムや通信衛星を用いた通信システムの構築を背景に、デジタル情報化されたソフトウェア（音声データ、映像データ等、以下、「コンテンツ」という）を各家庭等に配送するサービスが提案されている。このサービスシステムは、ビデオ・オン・デマンド方式等と呼ばれるデジタル・オーディオ・インタラクティブ・システムである。このデジタル・オーディオ・インタラクティブ・システムにおいては、サービス提供者とユーザとの間で電話線を介した通信が行われる。そして、サービス提供者は、ユーザから要求された時刻に要求された内容のコンテンツをこのユーザに配送するとともに、このソフトウェアの使用料金をクレジットカード会社等を通じて当該ユーザに課金し、その一部をコンテンツ供給者に還元するのである。

【0003】このようなデジタル・オーディオ・インタラクティブ・システムが普及してゆく上で重要な事は、インフラストラクチャーとなるサーバ/ネットワーク/ターミナルが低コストで構築されることは勿論であるが、これらを媒介としてユーザに提供されるコンテンツが豊富に準備されなければ、成功とはならないということである。即ち、コンテンツとインフラストラクチャーは車の両輪であるので、コンテンツ提供者がコンテンツ提供による利益回収を見込めるとともに不測の損害を被る危険がない仕組みをこのインフラストラクチャーに組み込むことにより、コンテンツが集まりやすい環境を整備することが不可欠なのである。なお、このような仕組みは、コンテンツ提供者とユーザとを媒介する供給メディアの種類（広帯域ケーブルネットワーク、衛星システム、移動通信、光メディアパッケージ等）に拘わらず、整備されていなければならない。

【0004】このような環境の整備がなされることにより、コンテンツ供給者は、安心して気軽に、コンテンツを供給することができるようになる。一方、ユーザは、いつでもどこでも、簡単な手続きによって必要なコンテンツを入手できるようになる。このことが、システムをより一層普及させるために重要なポイントとなっているのである。

【0005】一方、システム構築に当たっては、誰もが参加できるオープン性が重要であり、既存の標準技術を可能な限り活用する方式を取っていくことが必要である。また、技術の進歩や各種サービスの多様化に対応できる拡張性も持ち合わせたものであることを併せて考慮すべきである。

#### 【0006】

【発明が解決しようとする課題】以上説明したように、デジタル・オーディオ・インタラクティブ・システムにおいては、サービス提供者は、コンテンツ配送を要求してきたユーザが誰であるのかを正確に識別して、確実に課金することができなければならない。即ち、課金を行うために必要なデータ（例えば、クレジットカード番号、銀行口座番号、等）を登録していない第三者がこれらデータを登録しているユーザになりすましてコンテンツの配送を受けてしまうことを、防止しなければならない。そのため、登録されているIDコードとコンテンツ配送を行ったユーザのIDコードとを照合する認証システムが提案されている。

【0007】しかしながら、このようなIDコードによる認証システムでは、IDコードが第三者によって盗まれた場合においてこの第三者による盗用を防止する手ではない。なお、IDコードにパスワードを付する方式も提案されているが、盗まれた場合に第三者の盗用が可能であることには変わりがない。

【0008】そこで、本発明の第1の課題は、ユーザ（クライアント）とサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方において動的に作成することにより、第三者の盗用が不可能となるクライアント認証システムを提供することである。

【0009】また、単純なIDコードによって認証を行うシステムであるならば、ユーザがこのIDコードをマニュアルで入力できるので、コンテンツの配送要求を行った個人毎の認証も可能であるが、複雑な識別情報を扱う場合であると、識別情報の動的な作成は勿論、マニュアルによる識別情報の入力さえも不可能となってしまう。従って、従来提案されていた認証システムでは、コンテンツの再生を行う再生装置が自動的に認証作業を実行し、この再生装置毎に認証を行うようになっていた。

【0010】しかしながら、再生装置毎に認証を行うのであると、複数の再生装置を有している場合には、再生装置毎に課金のためのデータを登録しなければならない。また、自己の課金のためのデータがサービス提供者に登録されている場合であっても、例えば他人に借りた再生装置でコンテンツを再生することは一切できなくなってしまう。このように硬直したシステムであると、上述した理由によりシステム普及はおぼつかない。

【0011】そこで、本発明の第2の課題は、ユーザが容易に携帯できるとともに複数の再生装置に対して共通に装着できるモジュールに、認証を行うためのデータ及び機能を持たせたクライアント認証システムを提供することである。

#### 【0012】

【課題を解決するための手段】

(第1の課題を解決するための手段) 本発明によるクライアント認証システムの第1の態様は、上記第1の課題を解決するために、データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して配送されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証システムにおいて、前記データ供給装置は、前記クライアントに対応する第1の鍵を出力する鍵出力部と、前記クライアントからのアクセス要求に応じて乱数を発生する乱数発生手段と、前記鍵出力部において出力された第1の鍵によって前記乱数を暗号化することによって第1の認証子を出力する第1の暗号化手段と、前記クライアントに前記乱数を送信する第1の送信手段と、前記クライアントから第2の認証子を受信する第1の受信手段と、前記第1の認証子と前記第2の認証子とを比較して両者が一致している場合に当該クライアントからのアクセス要求であると認証する比較手段とを備え、前記クライアントは、前記データ供給装置にアクセス要求を行うアクセス要求手段と、前記データ供給装置から送信された前記乱数を受信する第2の受信手段と、前記第1の鍵と同一の第2の鍵を保持する鍵保持手段と、前記第2の鍵によって前記乱数を暗号化することによって前記第2の認証子を出力する第2の暗号化手段と、前記データ供給装置に前記第2の認証子を送信する第2の送信手段とを備えることを特徴とする(請求項1に対応)。

【0013】前記アクセス要求手段は、前記アクセス要求に際してそのクライアントに設定された固有の識別情報を前記データ供給装置に通知するとともに、前記鍵出力部は、各クライアントに固有の前記識別情報を加工することにより前記第1の鍵を生成するようにしても良い(請求項2に対応)。

【0014】前記データ供給装置は前記比較手段によって前記両認証子が一致すると判断された場合のみ前記データを前記クライアントに配送するようにしても良い(請求項3に対応)。

【0015】前記データ供給装置は暗号化された前記データを前記クライアントに配送するとともに、前記クライアントは前記暗号化された前記データを複合化する第1の復号化手段を備えるようにしても良い(請求項4に対応)。

【0016】前記データ供給装置は前記データを復号化するための第3の鍵を前記第1の鍵によって暗号化する第3の暗号化手段を備えているとともに、前記クライアントは前記暗号化された前記第3の鍵を前記第2の鍵によって復号化する第2の複合化手段を備え、前記第1の復号化手段はこの第2の複合化手段によって復号化された前記第3の鍵によって前記暗号化されたデータを復元するようにしても良い(請求項5に対応)。

【0017】前記データ供給装置は、前記暗号化されたデータを格納するための複数の格納装置を備えるとともに、

一方の格納装置に格納されている前記暗号化されたデータを前記第3の鍵を用いて復号化する第3の復号化手段と、第3の鍵を更新する鍵更新手段と、第3の復号化手段によって復号化されたデータを前記鍵更新手段によって更新された前記第3の鍵によって暗号化する第3の暗号化手段と、第3の暗号化手段によって暗号化されたデータを他の前記格納装置に格納する書込手段とを更に備えるように構成しても良い(請求項6に対応)。このように格納装置を二重化する事によりデータのバックアップができるとともに、暗号化した鍵をその都度更新するので、データのセキュリティを向上させることができる。

【0018】なお、前記第3の復号化手段、前記鍵更新手段、前記第3の暗号化手段、及び前記書込手段を一定時間毎に起動するようにしても良い(請求項7に対応)。本発明によるクライアント認証方法は、上記第1の課題を解決するため、データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して送出されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証方法において、前記クライアントは自己を識別する識別情報を付して前記データ供給装置にアクセス要求を行い、前記データ供給装置は、このアクセス要求に応じて乱数を発生してこの乱数を前記クライアントに送出するとともに、前記識別情報に対応する第1の鍵によって前記乱数を暗号化して第1の認証子に変換し、前記クライアントは前記第1の鍵と同一内容を有するものとして予め保持している第2の鍵によって前記乱数を暗号化して第2の認証子に変換するとともに、この第2の認証子を前記データ供給装置に送出し、前記データ供給装置は前記第1の認証子と前記第2の認証子とを比較して両者が一致した場合に前記クライアントからのアクセス要求があったことを認証することを特徴とする(請求項9に対応)。

(第2の課題を解決するための手段) 本発明の前記クライアント認証システムの第2の態様は、前記第1の態様におけるクライアントを、前記データを受信する本体部とこの本体部に対して着脱自在に設けられたモジュール部とから構成するとともに、少なくとも前記鍵保持手段及び前記第2の暗号化手段は前記モジュール部に備えるように構成したことを特徴とする(請求項8に対応)。なお、上述の識別情報を使用する場合には、この識別情報はこのモジュール部に格納しておく。また、上述の第1の複合化手段及び第2の複合化手段を設ける場合には、これら複合化手段をこのモジュール部に格納する。

【0019】

【作用】本発明の第1の態様によると、クライアントのアクセス要求手段がデータ供給装置にアクセス要求を行うと、このアクセス要求に応じて、データ供給装置の乱数発生部が乱数を発生するとともに、鍵出力部がこのクライアントに対応する第1の鍵を出力する。そして、第

1の通信手段は、アクセス要求元のクライアントに乱数を送信する。また、第1の暗号化手段は、鍵出力部において出力された第1の鍵によって乱数を暗号化することにより、第1の認証子を出力する。一方、クライアントの第2の受信手段が乱数を受信すると、第2の暗号化手段は、鍵保持手段が保持している前記第1の鍵と同一の第2の鍵によってこの乱数を暗号化することにより、第2の認証子を出力する。この第2の認証子は、第2の送信手段によってデータ供給装置に送信される。データ供給装置の第1の受信手段がこの第2の認証子を受信すると、比較手段が第1の認証子と第2の認証子とを比較して、両者が一致している場合に当該クライアントからのアクセス要求であると認証する。従って、通信インタフェース上で送信される識別のための情報（認証子）は暗号化されたものであって、その暗号化された結果は乱数に従って変化するので一定にはならない。そのため、第三者による盗用が不可能になる。

【0020】本発明の第2の態様によると、クライアントを構成する各構成部のうち、認証に必要なデータを保持する構成部（鍵保持手段）や認証に必要な処理を行うための構成部（第2の暗号化手段）のみを、本体部から着脱自在に設けたモジュール部に備えるようにしたので、誰の所有による本体部であっても、ユーザが自分のモジュール部を接続してデータの配送を受けることができる。

【0021】

【実施例】以下、図面に基づいて、本発明の一実施例の説明を行う。本実施例は、本発明によるクライアント認証システムを、デジタル・オーディオ・インタラクティブ・システムに適用したものである。なお以下の説明においては、コンテンツを再生するためのコンテンツ再生装置のことを、「サービスクライアント」という。

《実施例の構成》

（システムの全体構成）本実施例によるデジタル・オーディオ・インタラクティブ・システムを図1に示す。このシステムは、多数のコンテンツを格納するとともにこのコンテンツを配送するためのサービス提供者側システム1と、コンテンツを再生するための多数の端末とから、構成されている。この端末には、パーソナルコンピュータ2、サービスクライアント6a、6b、及びDVDプレーヤ8が含まれている。また、パーソナルコンピュータ2にはリムーバブルディスク装置3が接続されている。また、第1のサービスクライアント6aには、SCSIインタフェースを介して光磁気ディスクドライブ4が接続されている。DVDプレーヤ8を除く各端末は、上位サービスレイヤインタフェースS1、及びアプリケーションサービスレイヤインタフェースS2を介して、サービス提供者側システム1に接続されている。

【0022】これら上位サービスレイヤインタフェースS1、及びアプリケーションサービスレイヤインタフェ

ースS2は、図2に示すDAVIC 1.0システムリファレンスモデルによって定義されたインタフェースである。この上位サービスレイヤインタフェースS1は、コンテンツを配送するためのインタフェースであり、具体的には、ケーブルテレビジョンシステムのケーブル、衛星回線、ISDN等である。また、アプリケーションサービスレイヤインタフェースS2は、アクセス制御情報を交換するためのインタフェースであり、ケーブルテレビジョンシステムのケーブル、ISDNを上位サービスレイヤインタフェースS1と兼用することができる他、アナログ電話網を用いることができる。

【0023】なお、図1に示した（S1）は、物理的運搬を意味する。即ち、サービス提供者から購入したコンテンツ入りのフロッピーディスクを運搬して、パーソナルコンピュータ1のリムーバブルディスク装置3にロードしたり、サービス提供者から購入したコンテンツ入りのビデオディスクを運搬して、DVDプレーヤ8にロードすることを意味する。このような物理的運搬も、S1のインタフェースに該当する。同様に、制御情報をFAX、メール等によって送信することも、S2のインタフェースに該当する。

【0024】本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、コンテンツ提供者又はサービス提供者から提供される有料のコンテンツまたは機密情報を第三者から容易に傍受されることを防ぐ目的のために、サービス提供者側システム1とサービスクライアント6との間に、セキュリティ機構を設けた。このセキュリティ機構は、サービス提供者側システム1から供給されるコンテンツが第三者によって悪用されたり転用されることを防止するために、このコンテンツを暗号化してサービスクライアント6に提供する。即ち、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、図2に示したDAVIC 1.0システムリファレンスモデルに基づき、セキュリティ・アンド・アクセス・コントロール機能を、サービス提供者側システム1及びサービスクライアント6に置いたのである。

【0025】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、サービスクライアント6に復号化機能を持たせるために、模倣や改造が難しいハードウェア機構の一部採用し、認証及び秘匿を実現した。

【0026】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、ユーザへの利便性を考慮し、復号化機能を実現するアルゴリズム、鍵管理、認証、秘匿、および課金に関する情報などユーザのセキュリティに付随する機能を、利用者が携帯可能なモジュール（以後、「MASC: Media Access and Security Card」と呼ぶ）5に収め、このMASC 5をサービスクライアント6に脱着可能とした。そのた

め、このMASC5を何れかのサービスクライアント6に装着することにより、別個のサービスクライアント6であっても同様のサービスを享受することが可能となる。

【0027】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、他の標準化作業を尊重するため、サービスクライアント6側の認証方式は、ISO/IEC9798-2に準拠した。また、鍵管理方式は、B-MACスクランブル放送で採用されている方式に準拠した。また、暗号登録方式は、ISO/IEC 9979に準拠し、鍵サイズおよび入出力データサイズのみ規定するとともに処理アルゴリズムは規定しないものとした。また、MASC5のサービスクライアント6との物理インタフェースは、DVB方式案の一部を変更して採用した。

【0028】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、コンテンツ提供形態の多様化（ケーブル、衛星システム、パッケージ等）に対応できるように、拡張性の高いデータ構造、処理方式を採用した。

【0029】＜サービス提供者側システムの構成＞次に、図3を参照して、データ供給装置としてのサービス提供者側システム1の内部構成を説明する。図3に示すように、サービス提供者側システム1は、サーバ10と、このサーバ10と各々バス接続されたユーザプロフィール11、第1データファイル12、第2データファイル13、デジタル署名部14、認証部15、鍵更新処理部16、鍵管理部18、及び乱数発生器20と、サーバ10に夫々接続された衛星回線S、ケーブルテレビジョンシステムのケーブルC、及び電話網Nと、鍵更新処理部16に接続された鍵更新タイマ17と、鍵管理部18に接続されたサービスプロバイダID記憶部19とから、構成されている。

【0030】第1の送信手段及び第1の受信手段としてのサーバ10は、サービス提供者側システム1全体の制御を行うとともに、衛星回線S、ケーブルテレビジョンシステムのケーブルC、電話網Nを介してサービスクライアント6と通信を行う処理装置である。

【0031】ユーザプロフィール11は、各MASCのIDが登録されているデータベースである。第1データファイル12は、暗号化された多数のコンテンツ及びそれらのID（タイトルID）を格納するデータベースである。第2データファイル13は、この第1データファイル12に格納されていたコンテンツを別の鍵を用いて再暗号化したもの及びそれらタイトルIDを格納するデータベースである。即ち、これらのデータファイル12、13に格納されるコンテンツは、一定時間毎に再暗号化されて、一方のデータファイルから他方のデータファイルに移されるのである。なお、これらデータファイル12、13に格納されるコンテンツには、予めMPEG-2規格により圧縮処理がなされている。

【0032】デジタル署名部14は、ユーザに対する課金額に対応した一定範囲のコンテンツ再生を許可するデータを、このデータが正しいことを論理的に証明するデジタル署名情報を付して、サービスクライアント6に送信する部分である。

【0033】認証部15は、当該サービス提供者側システム1に対して通信を行ってきたサービスクライアントに装着された個々のMASC5がユーザプロフィール11にそのIDが登録されているどのMASC5であるのかを調べる作業を行う。

【0034】乱数発生手段としての乱数発生器20は、この認証部15の作業において用いられる乱数を発生する。鍵出力部としての鍵管理部18は、認証部15におけるMASKの識別に用いる鍵（第1の鍵）を、ユーザプロフィール11に登録されているMASCのIDから生成するとともに、各データファイル12、13に格納されている暗号化されたコンテンツを復元するための鍵（第3の鍵）を、対応するタイトルIDに基づいて生成する。

【0035】サービスプロバイダID記憶部19は、この鍵管理部18における鍵生成に用いられる当該サービス提供者側システムのID（サービスプロバイダID：IDP）を保持しているメモリである。

【0036】鍵更新処理部16は、一方のデータファイル12、13に格納されているコンテンツを鍵管理部18において生成されたタイトルIDに基づいて復元するとともに新たな鍵を作成し、復元されたコンテンツをこの新たな鍵によって暗号化して他方のデータファイル12、13に格納する。

【0037】鍵更新タイマ17は、この鍵更新処理部における処理のタイミングを規定するタイマである。

＜サービスクライアントシステムの構成＞次に、図4を参照して、サービスクライアントシステムの構成を説明する。

【0038】図4に示すように、サービスクライアントシステムは、衛星回線からの電波を受信するパラボラアンテナ22と、このパラボラアンテナ22に接続された衛星デコーダ23と、ケーブルテレビジョンシステムのケーブルに接続されたCATVアダプタ26と、光磁気ディスクドライブ4と、これら衛星デコーダ23、CATVアダプタ26、及び光磁気ディスクドライブ4に接続されたデータセクタ38と、このデータセクタ38に接続された本体部としてのサービスクライアント6と、このサービスクライアント6に装着されたモジュール部としてのMASC5と、電話網Nに接続されたモデム57とから、構成されている。

【0039】衛星デコーダ23は、パラボラアンテナ22によって受信された信号を復調する復調回路24と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ25とから、構成されている。デコーダ

25の出力端子は、データセクタ38の第1コネクタに接続される。

【0040】CATVアダプタ23は、ケーブルから受信された信号を復調する復調回路27と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ28とから、構成されている。デコーダ28の出力端子は、データセクタ38の第2コネクタに接続される。

【0041】光磁気ディスクドライブ4は、データセクタ38の第4コネクタに接続されたエンコーダ35と、このエンコーダ35によってエラー訂正及びビットの並び替えがなされたデータを変調する変調回路34と、光磁気ディスク30に対してデータの書込/読み出しを行うピックアップ31と、ピックアップ31によって読み出されたデータを復調する復調回路32と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ33と、光磁気ディスク30を回転させるとともにピックアップ31をトラッキングさせるドライブ回路36とから、構成されている。デコーダ33の出力端子は、データセクタ38の第3コネクタに接続される。

【0042】データセクタ38は、第1乃至第3コネクタから入力したデータを第4コネクタ又は第5コネクタに出力する。そのために、データセクタ38は、第1乃至第3の何れかのコネクタに接続線を接続するかを選択するスイッチSW1と、第4又は第5の何れかのコネクタに接続線を接続するかを選択するスイッチSW2とを備えている。

【0043】サービスクライアント6は、データセクタの第5コネクタに接続されたDL40、ホストCPU41、及びスイッチ42と、スイッチ42に接続されたデマルチプレクサ43と、このデマルチプレクサ43に接続された画像用MPEG伸長回路44と、この画像用MPEG伸長回路44に接続されたD/A変換器47と、デマルチプレクサ43に接続された音声用MPEG伸長回路45と、この音声用MPEG伸長回路45に接続されたD/A変換器48と、両MPEG伸長回路44、45に接続された同期回路46と、ホストCPU41に接続されたセクタペイロード対向テーブル49と、モデム57に接続されたインタフェース50とから、構成されている。

【0044】DL40は、ディレイライン装置であり、トグルバッファ又はFIFOメモリから構成された帯域変換装置である。スイッチ42はCPU41からの指示に従い、データセクタ38からの信号線又はMASC5からの信号線をデマルチプレクサ43に接続する。また、スイッチ42は、CPU41からの指示に応じて、回路を開く。

【0045】ホストCPU41は、当該サービスクライアント6全体の制御を行う制御装置である。また、ホス

トCPU41は、データセクタ38から受信したコンテンツが予め暗号化されているかどうかを解析する。そして、暗号化がなされていないのであればデータセクタ38からの信号線をデマルチプレクサ43に接続させる指示をスイッチ42に対して行い、暗号化がなされているのであればMASC5からの信号線をデマルチプレクサ43に接続させる指示をスイッチ42に対して行うとともに、MASC5に対して復号化を指示する。なお、ホストCPU41は、MASC5の制御CPU51からの指示があった場合には、コンテンツが暗号化されている場合であっても、スイッチ42に対してデータセクタからの信号線をデマルチプレクサ43に接続させる指示を行う。また、ホストSPU41は、データセクタ38からコンテンツを構成する各フレームを受信する毎に、MASC5に対して通知を行う。

【0046】デマルチプレクサ43は、コンテンツ中の音声データフレーム及び画像データフレームを分離する。そして、画像データフレームを画像用MPEG伸長回路(MPEG-2)44に出力し、音声データフレームを音声用MPEG伸長回路(MPEG-2)45に出力する。

【0047】MPEG伸長回路(MPEG-2)44、45は、MPEG規格で圧縮されたままの状態では送信されて来た画像データフレーム、又は音声データフレームを伸長して、画像又は音声出力可能なフォーマットに復元する回路である。これらMPEG伸長回路(MPEG-2)44、45においてデータフレームの伸長をする際には、同期回路46によって出力の同期がとられる。即ち、同期回路46から出力される同期信号に同期して、各MPEG伸長回路(MPEG-2)44、45は、伸長されたデータフレームを出力するのである。

【0048】画像用MPEG伸長回路(MPEG-2)44からの出力は、D/A変換器47によってアナログ信号に変換される。このアナログ信号は、当該サービスクライアント2に接続されている図示せぬTVモニタ装置に向けて出力される。また、音声用MPEG伸長回路(MPEG-2)45からの出力は、D/A変換器48によってアナログ信号に変換される。このアナログ信号は、当該サービスクライアントに接続されている図示せぬスピーカに向けて出力される。

【0049】セクタペイロード対応テーブル49は、光磁気ディスク30の各セクタとフレームとの関係を対応させているテーブルである。即ち、光磁気ディスクドライブ4からのコンテンツを読み出している場合において、ホストCPU41によって各フレームが読みとられる毎に、このセクタペイロード対応テーブル49によってセクタとの対応が調べられるのである。そして、現在のセクタから全てのフレームが読み出された時には、セクタコントローラ37に対して、ピックアップ31のトラッキングを行うべき旨が指示されるのである。

【0050】第2の受信手段及び第2の送信手段としてのインタフェース50は、モデム57と電話網N(S2)を介して、サービス提供者側システム1のサーバ10と通信を行い、制御情報の送受信を行う。

【0051】次に、DL40、ホストCPU51、スイッチ42、及びインタフェース56に接続されるMASC5の説明を行う。サービスクライアント6に提供される各種コンテンツは、衛星通信の様に入手が容易な通信媒体を介して配送されることがあるので、その再生に対する課金方法を如何にするかが問題となる。また、このような通信媒体を介して配送されるコンテンツは第三者による盗用を防止するために予め暗号化された状態で流通されるので、これを復号化する必要がある。そのため用いられるのがMASC5である。即ち、MASC5は、ホストCPU41からの指示に応じて、DL40を介して受信したコンテンツを復号化してスイッチ42に送信する。また、MASC5は、ホストCPU41がフレーム41を受信する毎に行う通知をカウントして、課金カウンタ値Xを減算する。この課金カウンタ値Xとは、ユーザがサービス提供者側システムのデジタル署名部14に対して代金支払いを了承することによって当該SD回路に書き込まれたポイントである。MASC5は、この課金カウンタ値Xが0になった時に、ホストCPU41に対して、スイッチ42を開かせるのである。

【0052】なお、このMASC5は、サービスクライアント6のカードスロット（たとえばPCMCIA準拠のカードスロット）内に着脱自在に装着されたICカードの形態で実現される。このようなICカードの形態にしておけば、SD回路の運搬が容易となる。

【0053】このMASC5は、相互にバス接続された制御CPU51、DES(Data Encryption Standard)53、課金情報記憶部55、ROM57、並びにI/O装置52、54、及び56から構成されている。

【0054】制御CPU51は、サービスクライアント6内のホスト制御CPU14に接続されており、ホストCPU41からの指示に応じてDES53に対して復号化処理を実行させる。また、制御CPU51は、ホストCPU41からのフレーム受信通知に応じて課金部55内に格納されている課金カウンタ値Xを減算するとともに、この課金カウンタ値Xが0になったときは、CPU41に対して、スイッチ42を開かせる。また、制御CPU51は、I/O装置56、インタフェース50及びモデム57を介してサービス提供者側システム1との間で通信を行って、アクセス要求、デジタル署名、及びユーザ認証のために必要な処理を行う（アクセス要求手段に対応）。

【0055】鍵保持手段としてのROM56は、この制御CPU51における処理に必要な諸データ（例えば、当該MASC5を識別するための識別ID<sub>i</sub>〔固有の識

別情報〕、当該MASC5に固有のものとして備えられた個別鍵K<sub>i</sub>〔第2の鍵〕）を記憶しているメモリである。

【0056】課金情報記憶部55は、上述した課金カウンタ値Xを格納しているメモリである。なお、課金情報記憶部55内において、課金カウンタ値Xは暗号化されている。従って、ユーザがこの課金情報記憶部55を解析して課金カウンタ値Xを書き換えることは、不可能である。

【0057】第2の暗号化手段、並びに第1及び第2の複合化手段としてのDES7は、I/O装置52を介してDL40から受け取ったコンテンツを復号化する機能、及び制御CPU51が行うデジタル署名及びユーザ認証に際して必要な暗号化及び復号化を行う機能を有する。DES7により復号化されたコンテンツ（画像フレーム、音声フレーム）は、I/O装置54を通じて、スイッチ42に送出される。

《実施例における処理内容》次に、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいて、サービス提供者側システム1とサービスクライアント6との間で実行される制御処理を、フローチャート及びこのフローチャートの各ステップにおいて実現される機能を示すための機能ブロック図を参照して、説明する。

【0058】サービスクライアント6がサービス提供者側システム1管理の情報にアクセスする場合、安全な通信制御手段が必要となる。これはサービスクライアント6とサービス提供者側システムとの間を結ぶS1とS2の形態により異なる。

【0059】（コンテンツ情報送信制御処理）先ず最初に、サービスクライアント6側からサービス提供側システム1に対して何れかのコンテンツの配送を要求する際の制御処理について説明する。この場合、S1、S2のインタフェースが秘密保持性が高い通信媒体であるか否かによって、制御を異にする。なぜならば、秘密保持性が低い通信媒体によってコンテンツを配送する場合には、第三者による盗用やデータ改ざんを防ぐために暗号化する処理が不可欠だからである。

【0060】＜秘密保持性が高い通信媒体によるコンテンツ情報供給制御＞図5は、S1、S2の形態を、例えば光ファイバケーブル（ケーブルテレビジョンシステムのケーブル、等）のように、データ盗聴やデータ改ざんが比較的困難な信頼できるネットワークとした場合における制御内容を示す。この場合、サービスクライアント6側の不正アクセスのみが問題となる。従って、アクセス権確立のための認証が重要となる。

【0061】この場合の運用手順の概略を説明すると、最初にユーザは、サービスクライアント6にMASC5を挿入する。すると、サービスクライアント6は、MASC5の識別ID(ID<sub>i</sub>)を読み取り、その識別ID



(ID<sub>j</sub>)をサービス提供者側システムへ通知する。すると、サービス提供者側システム1は、何れのMASC5であるかを認証する。次に、サービス提供者側システム1は、要求されたコンテンツをサービスクライアント6に向けて配送し、課金システムを動作させる。その結果、サービスクライアント6は、コンテンツを入手する。

【0062】[アクセス要求]図5における最初のステップ01では、サービスクライアント6は、サービス提供者側システム1に対してアクセス要求を行う。この前提として、サービスクライアント6が所有するMASC5には、モジュール固有の識別ID(ID<sub>j</sub>)、個別鍵K<sub>j</sub>、及び認証アルゴリズムEK(X)が安全に格納されている。

【0063】ユーザは、このMASC5を任意のサービスクライアント6へ接続し、図示せぬ操作キーを介してサービス提供者側システムの識別ID(サービスプロバイダID:ID<sub>p</sub>)を入力する。すると、図6(1)に示すように、サービスクライアント6は、サービス提供者側システムへのデータファイルアクセス要求コマンド、及びモジュール固有の識別IDに、サービス提供者側システムのデスティネーション[サービス提供者側システムの識別ID(ID<sub>p</sub>)とサービスクライアント6の識別ID(アドレス)とを結合したもの]を付して、S2インタフェースを介してサービス提供者側システム1に送信する。なお、この時、サービスクライアント5は、配送を求めるコンテンツのタイトルID(ID<sub>T</sub>)を、サービス提供者側システム1に送信する。

【0064】[認証処理]図5における次のステップ02では、サービス提供者側システム1によるサービスクライアントの認証処理を行う。このサービスクライアント認証は、当事者以外の第三者によるサービス提供者側システム1のデータファイルへの不正アクセス阻止を目的に実行される。ここでは、ISO/IEC 9798-2を利用し、当事者間で互いに共有する秘密の鍵データが同一であることにより認証を行う。

【0065】サービス提供者側システム1がアクセス要求をしたサービスクライアント6の正当性を認証する場合には、図6に示すような手順で認証処理を行う。尚、この認証のための通信は、S2インタフェースを介して行われる。

【0066】サービス提供者側システム1のサーバ10がサービスクライアント6からのアクセス要求を受信すると(1)、鍵管理部18内の第1鍵生成部(鍵出力部)182は、受信したMASC識別ID(ID<sub>j</sub>)がユーザプロフィール11に登録されていることを確認し、ユーザプロフィール11内の当該識別ID(ID<sub>j</sub>)を基に、プロバイダ管理の第1マスタ鍵81を使ってクライアント個別鍵(第1の鍵)K<sub>j</sub>を生成する。この第1マスタ鍵81は、MASC5内に格納されてい

る個別鍵(第2の鍵)K<sub>j</sub>が生成された際に用いられたマスタ鍵と同一である。従って、受信したMASC識別ID(ID<sub>j</sub>)とユーザプロフィール11内に登録されている識別ID(ID<sub>j</sub>)とが同一である限り、MASC5内の個別鍵K<sub>j</sub>と全く同じクライアント個別鍵K<sub>j</sub>が生成されることになる。

【0067】これと同時に、サービス提供者側システム1内の乱数発生部20は、乱数Rを発生する。この乱数Rは、認証部15に入力されるとともに、サーバ10にも入力される。サーバ10は、この乱数Rにサービスクライアント向けデスティネーション[サービスクライアント6の識別ID(アドレス)とサービス提供者側システムの識別ID(ID<sub>p</sub>)とを結合したもの]を付けて、サービスクライアント6へ送信する(2)。

【0068】サービス提供者側システム1からの情報を受信したサービスクライアント6は、情報に含まれる乱数RをMASC5に与える。すると、MASC5は、MASC識別ID(ID<sub>j</sub>)に乱数Rを結合して、これを個別鍵K<sub>j</sub>によって暗号化することにより、第2の認証子を生成する。サービスクライアント6は、この第2の認証子にサービス提供者側システムのデスティネーションを付して再びサービス提供者側システム1へ送り返す(3)。

【0069】このクライアント情報を受信したサービス提供者側システム1は、この情報に含まれる第2の認証子を、認証部15内の比較器(比較手段)152へ設定する。更に、認証部15内の第1暗号化部(第1の暗号化手段)151は、サービスクライアント5から受信したMASC識別IDと乱数発生部20から受信した乱数Rとを結合して、これを鍵生成部182にて生成されたクライアント個別鍵K<sub>j</sub>によって暗号化することにより、第1の認証子を生成する。第1暗号化部151は、この第1の認証子を比較器152へ設定して、先に設定した第2の認証子と比較させる。比較器152において両認証子が一致すれば、サービスクライアント5及びサービス提供者側システム1間に同一の個別鍵K<sub>j</sub>が保有されていることになるので、認証部15は、当該サービスクライアントを通信当事者として認証し、後の処理を可能とする。これに対して、両認証子が相違している場合には、そのMASC5に対応する課金用データが登録されていないサービスクライアントであると判断して、後の処理を禁止する。このように、本実施例による認証方式によると、認証の対象となる個別鍵K<sub>j</sub>自体がインタフェース上を送信されるのではなく、アクセス要求の都度生成される乱数をこの個別鍵K<sub>j</sub>で暗号化した認証子が送信されるだけである。従って、第三者が乱数Rを盗んだとしても、個別鍵K<sub>j</sub>の内容を知らない限り、認証子を生成することは不可能である。また、認証子自体を盗んだとしても、既に正規のユーザに対する認証が済んでいる場合には、この認証子に対する乱数Rは認証

部15にセットされていないので、当該認証子は既に無効となっている。このように何れにしても第三者の不正なアクセスは、阻止されるのである。

【0070】なお、サービスクライアント6がサービス提供者側システム1を認証するときには、上記のサービスクライアント6及びサービス提供者側システム1の立場を入れ換えて同様な手順を実行することにより、サービスクライアント6がサービス提供者側システム1を認証することが可能となる。

【0071】また、認証プロセスで用いるパラメータは、認証子の生成アルゴリズムにより異なる。例えば生成アルゴリズムにDES (DATA ENCRYPTION STANDARD)を採用した場合、以下の通りである。

【0072】

乱数R : 32 ビット

MASC識別ID: 32 ビット (ECB入力時には残り32ビットはパディングする)

個別鍵K<sub>j</sub> : 56 ビット

マスタ鍵KM : 168ビット (56 ビット×3)

サービス提供者側システム1の利用モード: TRIPPLE ECB (ELECTRONIC CODE BOOK) (個別鍵生成, 乱数生成)

サービスクライアントの利用モード: ECB (認証処理)

【コンテンツ情報配送処理】図5における次のステップ03では、サービスクライアント6からのコンテンツ情報配送処理を行う。即ち、サービス提供者側システム1は、サービスクライアント5から要求されたタイトルID (IDT) に対応するコンテンツ (暗号化コンテンツ) を、何れかのデータファイル12, 13から読み出して復号化する。そして、S1インタフェースを介して、復号化されたコンテンツをサービスクライアント6に送信するのである。

【0073】コンテンツを受け取ったサービスクライアント6は、これを一旦光ディスクドライブ4に送信して光ディスク30に書き込むか、そのままCPU42に流す。ホストCPU42はこのコンテンツが暗号化されていないものであると解析して、スイッチ43をデータセレクト側に切り換える。従って、コンテンツはそのままデマルチプレクサ43にて画像フレームと音声フレームに分離されて、夫々MPEG伸長回路44, 45にて伸長され、DA変換器47, 48にてアナログ信号に変換される。そして、画像信号は図示せぬTVモニターへ送信され、音声信号は図示せぬスピーカへ送信される。

【0074】また、ホストCPU41は、コンテンツを構成する各フレームを読み込む毎に、MASC5内の制御CPU51に通知を行う。この制御CPU51は、通知の数をカウントして、課金情報記憶部55内の課金カウント値Xを減算する。そして、この課金カウント値Xが0になると、制御CPU51は、ホストCPU41に対して、スイッチを42を開かせる。従って、課金額に対応する使用許可量を越えたコンテンツの使用が阻止さ

れるのである。

【0075】＜一般のネットワークによるコンテンツ情報供給制御＞図7は、S1, S2の形態を、無線路や様々な迂回路を経由する一般のネットワーク形態とした場合における制御内容を示す。この形態では、データ盗聴やデータ改ざん行為が十分起こり得るので、上述のサービスクライアント認証処理の他、データ暗号化を如何に行うかが重要である。

【0076】この場合の運用手順の概略を説明すると、最初に利用者は、サービスクライアント6にMASC5を挿入する。すると、サービスクライアント6は、MASC5の識別ID (ID<sub>j</sub>) を読み取り、その識別ID (ID<sub>j</sub>) をサービス提供者側システム1へ通知する。すると、サービス提供者側システム1は、何れのMASC5であるかを認証する。次に、サービス提供者側システム1は、サービスに必要な鍵 (KG<sub>j</sub>) をサービスクライアント6に配送する。このようにして、サービスクライアント6は、必要な鍵 (KG<sub>j</sub>) を入手する。その後、サービス提供者側システム1は、要求されたコンテンツをサービスクライアント6に向けて配送し、課金システムを動作させる。その結果、サービスクライアント6は、この鍵 (KG<sub>j</sub>) を利用してコンテンツを入手する。

【0077】【アクセス要求】図7における最初のステップ11では、サービスクライアント6は、図8に示すように、サービス提供者側システム1に対してアクセス要求を行う。このアクセス要求の内容は、図5におけるステップ01と同じなので、その説明を省略する。

【0078】【認証処理】図7における次のステップ12では、サービス提供者側システム1は、図8に示すように、サービスクライアント6の認証を行う。この認証処理は、図5におけるステップ12と同じなので、その説明を省略する。

【0079】【鍵配送処理】図7における次のステップ13では、サービス提供者側システム1は、図8に示すように、暗号化コンテンツの復元用の鍵 (KG<sub>j</sub>) の配送を行う。この鍵配送は、暗号化されている各種コンテンツの情報をサービスクライアント6側で円滑に復号させる為に、S2インタフェースを使って行われる。

【0080】即ち、サービス提供者側システム1は、サービスクライアント6に装着されたMASC5が発信してきたMASC識別ID (ID<sub>j</sub>) から、クライアント個別鍵K<sub>j</sub>を生成する (このクライアント個別鍵K<sub>j</sub>としてクライアント認証において用いたものを流用しても良い)。サービス提供者側システム1は、クライアント個別鍵K<sub>j</sub>によってサービスプロバイダID (IDP) 及びタイトル鍵KG<sub>1j</sub>を暗号化し、サービスクライアント向けデスティネーション [サービスクライアント6の識別ID (アドレス) とサービス提供者側システム1の識別ID (アドレス) とを結合したもの] を付して、

MASC5に送信する。サービス提供者側システム1からの暗号化鍵情報は、MASC5において復号化され、タイトル鍵KG1jが得られる。以後、S1インタフェースで送られてくる暗号化コンテンツが、このタイトル鍵KG1jによって復号化される。

【0081】この鍵配送処理の内容を、図9の機能ブロック及び図10のサブルーチンフローチャートに基づいて説明する。なお、説明の都合上、現時点において第1データファイル12に暗号化コンテンツが格納されているとし、これを「旧データファイル」と称するものとする。

【0082】図10において、最初のステップ21では、サービス提供者側システム1の鍵管理部18内に備えられたスイッチSW4を、旧データファイル12側に切り換える。そして、サービスクライアント5から要求されているタイトルに対応するタイトルID(IDT)を、スイッチSW4を介して旧データファイル12から読み出す。第2鍵生成部184は、読み出したタイトルID(IDTj)を第2マスタ鍵185に基づいて暗号化し、タイトル鍵(第3の鍵)KG1jを生成する。

【0083】次のステップ22では、鍵管理部18内の第2暗号化部(第3の暗号化手段)183は、サービスプロバイダID記憶部19から受信したサービスプロバイダID(IDP)と、第2鍵生成部184から受信したタイトル鍵KGjとを、結合する。そして、第2暗号化部183は、認証処理時において第1鍵生成部182が生成したクライアント個別鍵Kjに基づいて、これらサービスプロバイダID(IDP)及びタイトル鍵KG1jを暗号化し、サーバ10に転送する。サーバ10は、受け取ったサービスプロバイダID及びタイトル鍵KG1jの暗号化情報を、S2インタフェースを介してサービスクライアント6に配送する。

【0084】次のステップ23では、サービスクライアント6は、サービスプロバイダID及びタイトル鍵KG1jの暗号化情報をMASC5に配送する。MASC5内の第1復号化部(第2の復号化部)101(DES53)は、MASC6のROM57に内蔵されている個別鍵Kjを用いてこの暗号化情報を復号化し、サービスプロバイダID及びタイトル鍵KG1jを獲得する。そして、このサービスプロバイダID(IDP)を比較器102にセットする。

【0085】次のステップ24では、MASC6内の比較器102は、第1復号化部101によってセットされたサービスプロバイダID(IDP)とアクセス要求時に図示せぬ操作キーを介して入力されたサービスプロバイダID(IDP)103とを、比較する。そして、両者が一致している場合には、処理をステップ25に進め、不一致の場合には、処理をステップ27に進める。

【0086】ステップS27において、受信不可能である旨がサービスクライアント5側に通知され、S2イン

タフェースを介してサービス提供者側システム1のサーバ10に転送される。

【0087】次のステップ28では、サービス提供者側システム1のサーバ10は、第2暗号化部183から受け取ったサービスプロバイダID(IDP)及びタイトル鍵KG1jの暗号化情報を、S2インタフェースを介して再度MASC5側へ配送する。その後、処理はステップS23に戻される。

【0088】これに対して、ステップ25では、MASC6内のスイッチSW3が閉じられ、第1復号化部101において復元されたタイトル鍵KG1jが第2復号化部(第1の復号化手段)104(DES53)にセットされる。それとともに、受信可能である旨がサービスクライアント5側に通知され、S2インタフェースを介してサービス提供者側システム1のサーバ10に転送される。

【0089】ステップ26において、サービス提供者側システム1のサーバ10は、スイッチSW1を閉じて、データファイル12からタイトル鍵KG1jに対応するタイトルの暗号化コンテンツを読み出す。

【0090】[コンテンツ情報配送処理] 図7のステップ14において実行されるコンテンツ情報配送処理は、図10のステップ26の直後に実行される。

【0091】即ち、図11に示すように、サーバ10は、データファイル12から読み出した暗号化コンテンツを、S1インタフェースを介してサービスクライアント6に配送する。サービスクライアント6は、この暗号化コンテンツをMASC5に転送する。MASC5の第2復号化部104(DES53)は、セットされたタイトル鍵KG1jを用いてこの暗号化コンテンツを復号化する。

【0092】図4を用いてこの復号化を具体的に説明する。コンテンツを受け取ったサービスクライアント6は、これを一旦光ディスクドライブ4に送信して光ディスク30に書き込むか、そのままCPU42に流す。ホストCPU42はこのコンテンツが暗号化されているものであると解析して、スイッチ43をMASC側に切り換えるとともに、MASC5の制御CPU51に対して、復号化処理を指示する。この指示に応じて、制御CPU51は、暗号化コンテンツをDL40及びI/O装置52を介して読み込み、DES53(第1復号化部101, 第2復号化部104)によって復号化を行う。このDES53には、インタフェース50及びI/O装置56を介して受信したタイトル鍵KG1jがセットされているので、このタイトル鍵KG1jを用いて複合化する。複合化されたコンテンツは、I/O装置54を介してスイッチ42に送信される。

【0093】コンテンツは、スイッチ42からデマルチプレクサ43に転送され、このデマルチプレクサ43にて画像フレームと音声フレームに分離されて、夫々MP

EG伸長回路44、45にて伸長され、DA変換器47、48にてアナログ信号に変換される。そして、画像信号は図示せぬTVモニタへ送信され、音声信号は図示せぬスピーカへ送信される。

【0094】また、ホストCPU41は、コンテンツを構成する各フレームを読み込む毎に、MASC5内の制御CPU51に通知を行う。この制御CPU51は、通知の数をカウントして、課金情報記憶部55内の課金カウント値Xを減算する。そして、この課金カウント値Xが0になると、制御CPU51は、DES53による復号化を中止するとともに、ホストCPU41に対してスイッチを42を開かせる。従って、課金額に対応する使用許可量を越えたコンテンツの使用が阻止されるのである。

【0095】このように、本実施例のキー配送処理によれば、データファイル12に格納されている各コンテンツ毎に、別個の復元用鍵（タイトル鍵KG1j）を生成した。従って、同一のユーザが同じキーを用いて他のタイトルのコンテンツを再生することが防止できる。また、このタイトル鍵KG1jは、MASC5毎に用意された鍵（個別鍵Kj）によって暗号化されるので、第三者が暗号化された鍵を傍受したとしても、タイトル鍵KG1jを復元することは不可能である。従って、第三者の盗用が阻止できる。

【0096】（ローカル課金処理）次に、コンテンツ情報を再生するために必要な課金カウント値Xの加算を申込むためのローカル課金処理を、図12に基づいて説明する。この課金カウント値Xの加算値は、サービスクライアント6からサービス提供者側システム1に対して、代金の銀行口座からの引き落としを条件に申し込まれ、サービス提供者側システム1によってMASC5に書き込まれる。このように、本実施例では、課金カウント値Xの管理をMASC5において行っているため、特にデータ改ざん防止に重点が置かれる。よって、サービス供給者側システム1がこの加算値の正当性を証明するために加算値情報に付すデジタル署名が重要となる。従って、サービス提供者側システム1には、予め、MASC5毎に、暗証番号が登録されているものとする。

【0097】【アクセス要求】図12における最初のステップ31では、サービスクライアント6は、図13に示すように、サービス提供者側システム1に対してアクセス要求を行う。このとき、サービスクライアント6は、サービス提供者側システム1への課金カウント値増加要求コマンド、及びMASC固有の識別IDに、サービス提供者側システムのデスティネーション（サービス提供者側システムの識別ID（サービスプロバイダID：IDP）とサービスクライアント6の識別ID（アドレス）とを結合したもの）を付して、S2インタフェースを介してサービス提供者側システム1に送信する。

【0098】【認証処理】図12における次のステップ

32では、サービス提供者側システム1は、図13に示すように、サービスクライアント6の認証を行う。この認証処理は、図5におけるステップ02と同じなので、その説明を省略する。

【0099】【デジタル署名処理及び課金カウント値の書込処理】図12における次のステップ33では、サービスクライアント6においてデジタル署名が行われ、次のステップ34では、サービス提供者側システム1による課金カウント値Xの補充処理が行われる（図13参照）。

【0100】即ち、ユーザによるメッセージの認証は、サービス提供者側システム1とサービスクライアント5との間で、課金に関わるセンシティブデータをやりとりするときに、通信路上での第三者によるデータの改竄行為やサービスクライアント6でのユーザによるデータ改竄行為を阻止し、当事者間で円滑なトランザクション行為を達成するために、用いられる。ここでは、ISO 8731-1に基づくMAC（MESSAGE AUTHENTICATION CODE）方式を利用する。

【0101】サービス提供者側システム1のデジタル署名部14は、ユーザの銀行口座から引き落とす金額に対応する補充カウンタ値のデータブロック（DATA OF MENEY）140を、送信用フレームFに格納する。補充カウンタ値のデータブロック（DATA OF MENEY）140は、また、当該MASC5についての加算履歴回数に応じてインクリメントされる通番（IV）によって署名処理される（ステップ33）。即ち、排他OR回路142及び第3暗号化部143において、暗証番号（IV）を用いて、補充カウンタ値のデータブロック（DATA OF MENEY）140が暗号化されるのである。このような署名処理の最終処理結果（MAC）は、サービス提供者側システム1が補充カウンタ値の正当性を証明するためのデータとして、送信用フレームFに格納される。この送信用フレームFは、S2インタフェースを介して、サービスクライアント6に装着されたMASC5に送信される（ステップ34）。

【0102】MASC5は、受信した送信用フレームFに対して、サービス提供者側システム1側と同一処理を行う。即ち、送信用フレームFから補充カウンタ値のデータブロック（DATA OF MENEY）140を読み出す。そして、排他OR回路106及び暗号化回路106（DES53）において、補充履歴回数に応じてインクリメントされる通番（IV）を用いて、補充カウンタ値データブロックの全てに対して署名処理を行う。なお、この通番（IV）は、通常であれば、サービス提供者側システム1のデジタル署名部14に格納されている通番（IV）に同期している。次に、比較器107において、署名処理の結果生成されたMACの値（MAC'）と送信用フレームFに格納されたMAC141の値とを比較する。比較の結果、両値が一致した時には、送信用フレ

ムFに格納された補充カウンタ値のデータブロック (DATA OF MONEY) 140が正しい金額データであると判断し、スイッチSW6を閉じる。すると、この補充カウンタ値が、課金情報記憶部55に格納されている課金カウンタ値Xに加算される。

【0103】以上の結果、ユーザが送信用フレームFから補充カウンタ値を読み出してこれを書き換えた場合には、この書き換えた補充カウンタ値が課金カウンタ値Xに加算できなくなってしまうので、不正が防止できる。

【0104】このデジタル署名処理に用いられるパラメータは以下の通りである。

暗号化処理 : DES  
署名鍵 : 56ビット  
MAC : 32ビット(64ビット出力の左32ビットを抽出)  
金額データ : 64ビットブロック単位(不足分の32ビットはパディングビットを挿入)

(鍵の更新処理) 次に、一定時間毎に、旧データファイル12に格納されたコンテンツを新規なタイトル鍵KG<sub>2j</sub>によって暗号化し直して新データファイル13に格納するための処理を図9のブロック図及び図14のフローチャートを参照して説明する。

【0105】即ち、サービス提供者側システム1で管理する各種タイトルのコンテンツは、それぞれのタイトル鍵KG<sub>1j</sub>で予め暗号化されているが、同一の鍵で恒久的に暗号化した場合、解読の危険性が高まる。この為、タイトル鍵KG<sub>1j</sub>の定期的更新を行って、暗号化をし直す必要があるのである。また、新たに追加されたタイトルのコンテンツに対しても、その都度タイトルに応じたタイトル鍵KG<sub>2j</sub>で暗号化する必要がある。そのため、本実施例では、データファイルを第1のデータファイル12及び第2のデータファイル13に分け、一方のデータファイルに現在稼働中の暗号化情報を格納するとともに(旧データファイル)、他方のデータファイルには図14の鍵の更新処理を実行することにより新たな暗号化コンテンツを格納するのである(新データファイル)。この図14の処理の前提として、鍵管理部18の第2マスターキー185と鍵更新処理部16の第2マスター鍵163とは全く同じものであるとする。また、一度使用したタイトル鍵KG<sub>1j</sub>は再使用を行うことなく使い捨てられるので、タイトル鍵KG<sub>1j</sub>の生成に用いられる第2マスター鍵163、185は、鍵更新の都度変更される。

【0106】図14の処理は鍵更新タイマ17に設定された周期毎にスタートする。即ち、本実施例では、タイトル鍵KG<sub>1j</sub>の更新を、プログラムのサイクル及び安全係数を考慮に入れ、例えば一週間毎に行うようにしている。なお、図14の処理のスタートタイミング、即ち、新タイトル鍵KG<sub>2j</sub>によって暗号化され直した新コンテンツの新データファイルへ格納するタイミングは、旧データファイル稼働中であることは、言うまでもない。ま

た、第1データファイル12を旧データファイルとする場合には、スイッチSW1を閉じ、スイッチSW2を開き、スイッチSW4を第1データファイル12側とし、スイッチSW5を第2データファイル側13とする。これに対して、第2データファイル13を旧データファイルとする場合には、これらと全く逆にする。

【0107】図14の処理において最初のステップ41では、鍵更新処理部16の復号処理部(第3の復号化手段)161に、第2鍵生成部184において現在のタイトルID(IDT<sub>1j</sub>)に基づいて生成されたタイトル鍵KG<sub>1j</sub>をセットする。

【0108】次のステップ42では、旧データファイル12に格納されている当該タイトル鍵KG<sub>1j</sub>に対応する暗号化コンテンツを鍵更新処理部16の復号装置161にセットして、タイトル鍵KG<sub>1j</sub>に基づいて復号を行う。

【0109】次のステップ43では、鍵更新処理部16の第3鍵生成部(鍵更新手段)164は、新データファイルに予め格納されている何れかのタイトルID(IDT<sub>2j</sub>)を第2マスター鍵163により暗号化して、新タイトル鍵KG<sub>2j</sub>を生成する。第4暗号化部(第3の暗号化手段)162は、復号されたコンテンツを新タイトル鍵KG<sub>2j</sub>に基づいて暗号化し直す。

【0110】次のステップ44では、第4暗号化部162が暗号化し直した暗号化コンテンツを、新データファイル13に書き込む(書込手段に対応)。次のステップ45では、鍵更新タイマ17によってある期限(例えば毎日曜日の深夜以降)まで待ち、各スイッチSW1、2、4、5を切り換える。例えば、第1データファイルを旧ファイルとしていた場合においては、スイッチSW2を閉じ、スイッチSW1を開き、スイッチSW4を更新側に切り換え、スイッチSW5を旧データファイル12側に切り換える。これより、新データファイル13に格納されているタイトルID(IDT<sub>2j</sub>)を鍵管理部18に送信可能となり、新データファイル13に格納されている暗号化コンテンツをサーバ10に送信可能となるとともに、この新データファイルを旧データファイルとして扱う次の更新処理が可能となる。このステップ44の処理が完了すると、処理が図10のステップ21に渡される。

【0111】(MASCの緊急対策) ユーザ側で万一MASC5の紛失又は盗難に遭遇した場合、サービス提供者は、緊急に鍵の破壊及びMASK5の再発行を行う。即ち、ユーザは、MASC5の紛失又は盗難の事実が確認されたなら、電話等の通信手段を使って直ちにサービス提供者にそのむね連絡する。このときユーザは、自身の名前、住所、連絡先をサービス提供者に通知する。次に、サービス提供者は、サービス提供者側システム1のプロファイルデータでユーザを確認後、ユーザに対して電話によるコールバックを行う。そして、サービス提供

者及びユーザ間で確認及び合意がとれれば、サービス提供者は、プロフィールから該当ユーザデータ全てを抹消し、対応するMASC5のID(ID<sub>i</sub>)を永久欠番とする。その後、ユーザは、サービス提供者又は近くの特約店或いは代理店へ行き、再登録の申請を行い、新しいID(ID<sub>j</sub>)付MASC5を発行してもらう。

【0112】

【発明の効果】以上のように構成された本発明のクライアント認証システムの第1の態様によると、ユーザ(クライアント)とサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方において動的に作成するので、第三者の盗用が不可能となる。

【0113】また、本発明のクライアント認証システムの第1の態様によると、ユーザが容易に携帯できるとともに複数の再生装置に対して共通に装着されるモジュールに、認証を行うためのデータ及び機能を持たせることができるので、再生装置が自己のものか否かに拘わらずコンテンツを再生できるとともに、サービス提供者は確実にコンテンツ再生代金を徴収することができる。

【図面の簡単な説明】

【図1】 本発明の一実施例によるクライアント認証システムが適用されたデジタル・オーディオ・インタラクティブ・システムの概略図

【図2】 図1のデジタル・オーディオ・インタラクティブ・システムに対応するシステムリファレンスモデルを示す図

【図3】 図1のサービス提供者側システムの構成を示すブロック図

【図4】 図1のサービスクライアント側システムの構成を示すブロック図

【図5】 秘密保持性が高い通信媒体によるコンテンツ情報供給制御を示すフローチャート

【図6】 認証処理に関連する構成を示すブロック図

【図7】 一般のネットワークによるコンテンツ情報供給制御を示すフローチャート

【図8】 鍵配送処理を示すタイムアロー図

【図9】 鍵配送処理に関連する構成を示すブロック図

【図10】 鍵配送処理の内容を示すフローチャート

【図11】 コンテンツ配送処理を示すタイムアロー図

【図12】 ローカル課金処理の内容を示すフローチャート

【図13】 デジタル署名処理に関連する構成を示すブロック図

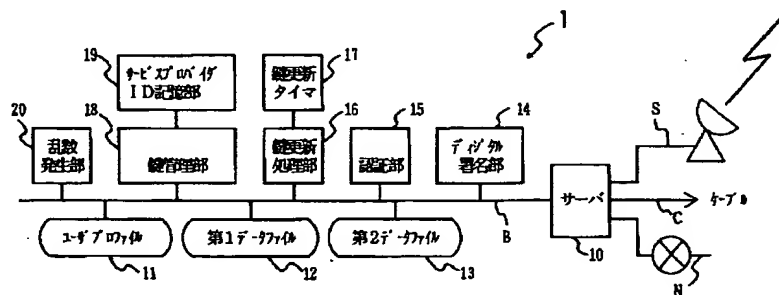
【図14】 鍵の更新処理の内容を示すタイムアロー図

【符号の説明】

- 1 サービス提供者側システム
- 5 MASC
- 6 サービスクライアント
- 10 サーバ
- 11 ユーザプロフィール
- 12 第1データファイル
- 13 第2データファイル
- 14 デジタル署名部
- 15 認証部
- 16 鍵更新処理部
- 18 鍵管理部
- 20 乱数発生器
- 53 DES
- 55 課金情報記憶部
- 57 ROM

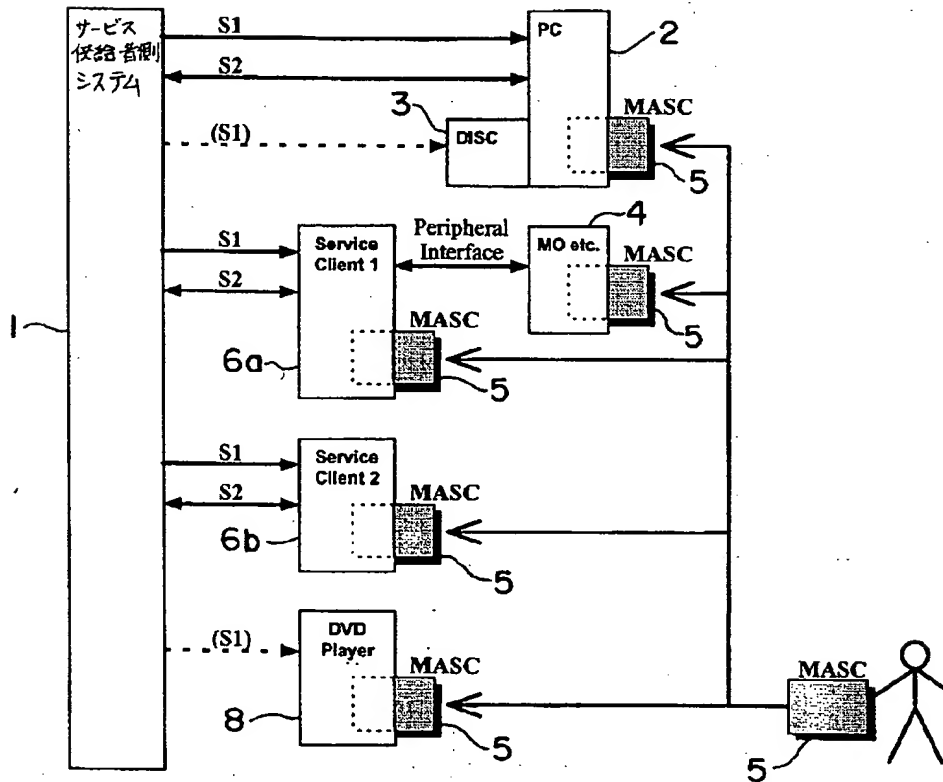
【図3】

図1のサービス提供者側システムの構成を示すブロック図



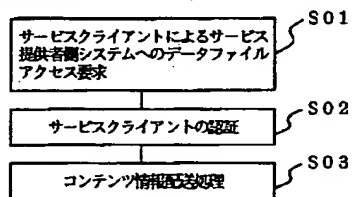
【図1】

本発明の一実施例によるクライアント認証システムが適用されたデジタル・オーディオ・インタラクティブ・システムの概略図



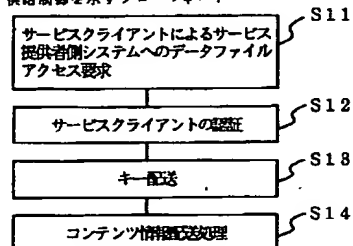
【図5】

秘密保持性が高い通信媒体によるコンテンツ情報供給制御を示すフローチャート



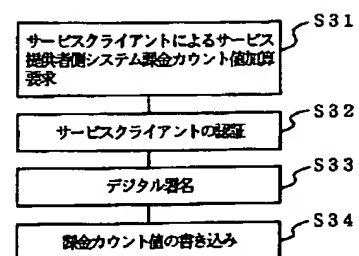
【図7】

一般のネットワークによるコンテンツ情報供給制御を示すフローチャート



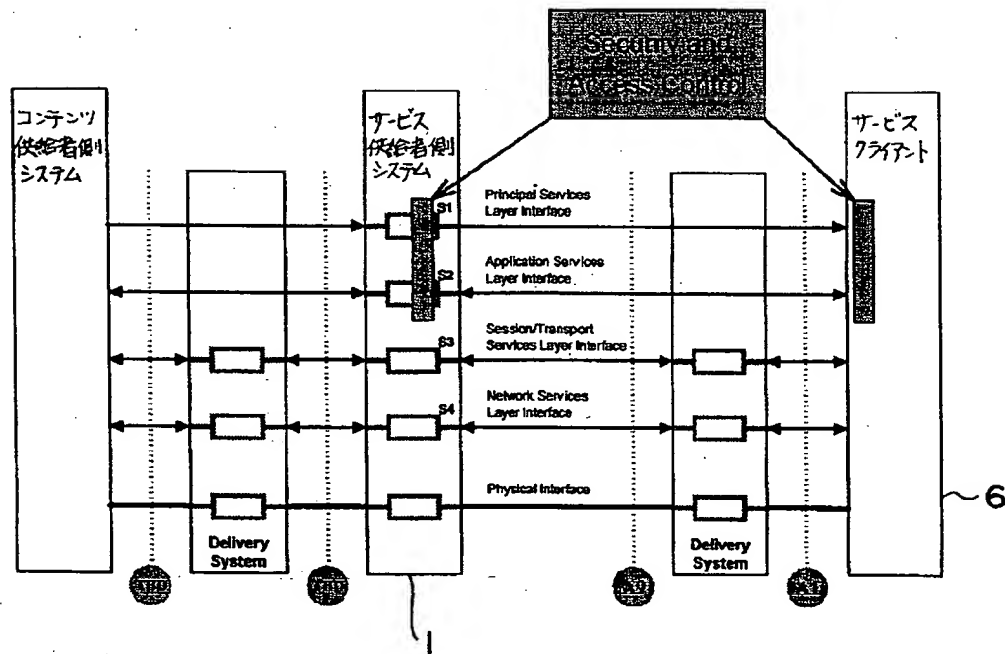
【図12】

ローカル課金処理の内容を示すフローチャート



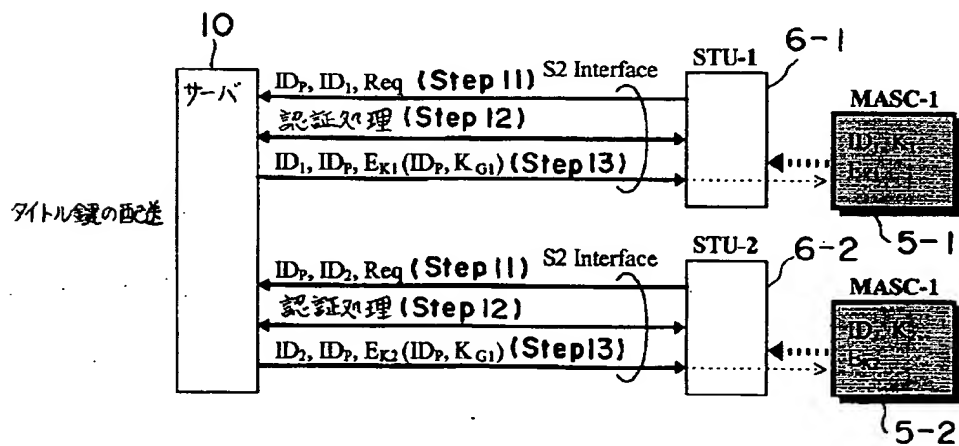
【図2】

図1のデジタル・オーディオ・インタラクティブ・システムに対応するシステムリファレンスモデルを示す図



【図8】

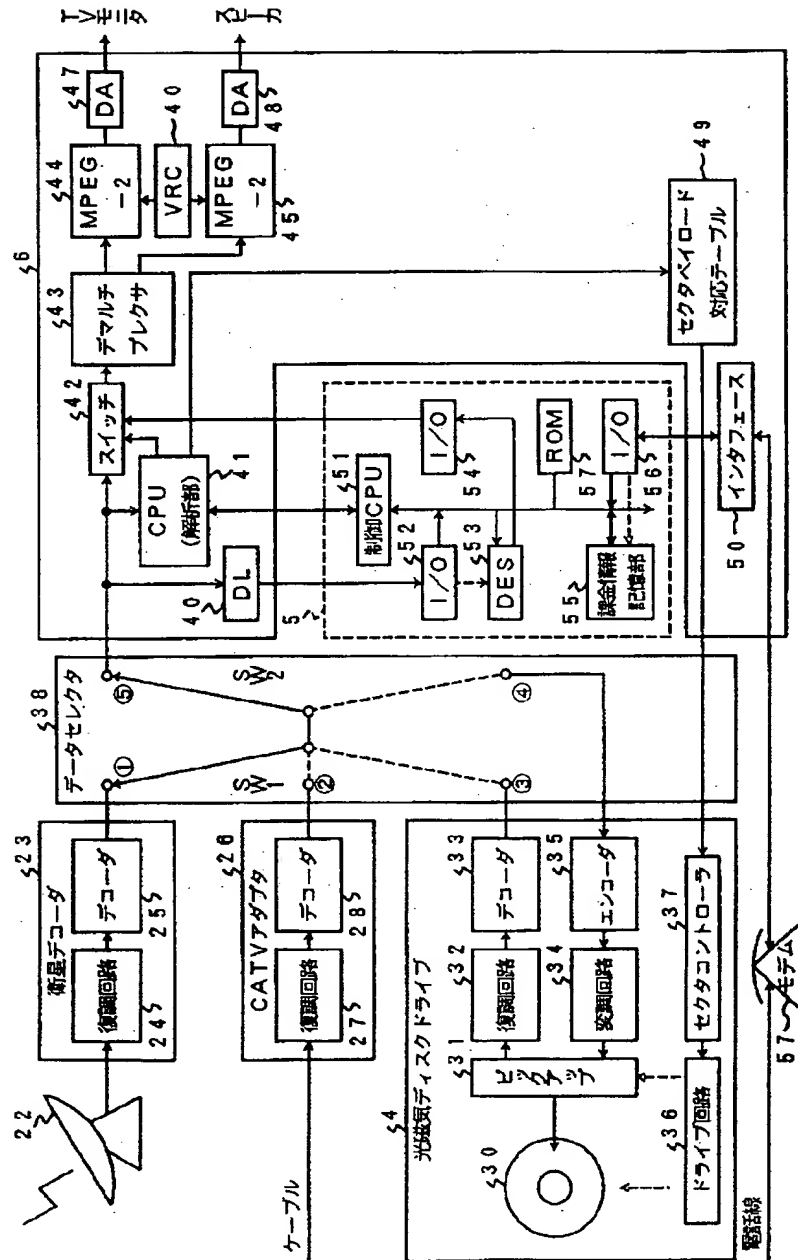
鍵配送処理を示すタイムアロー図



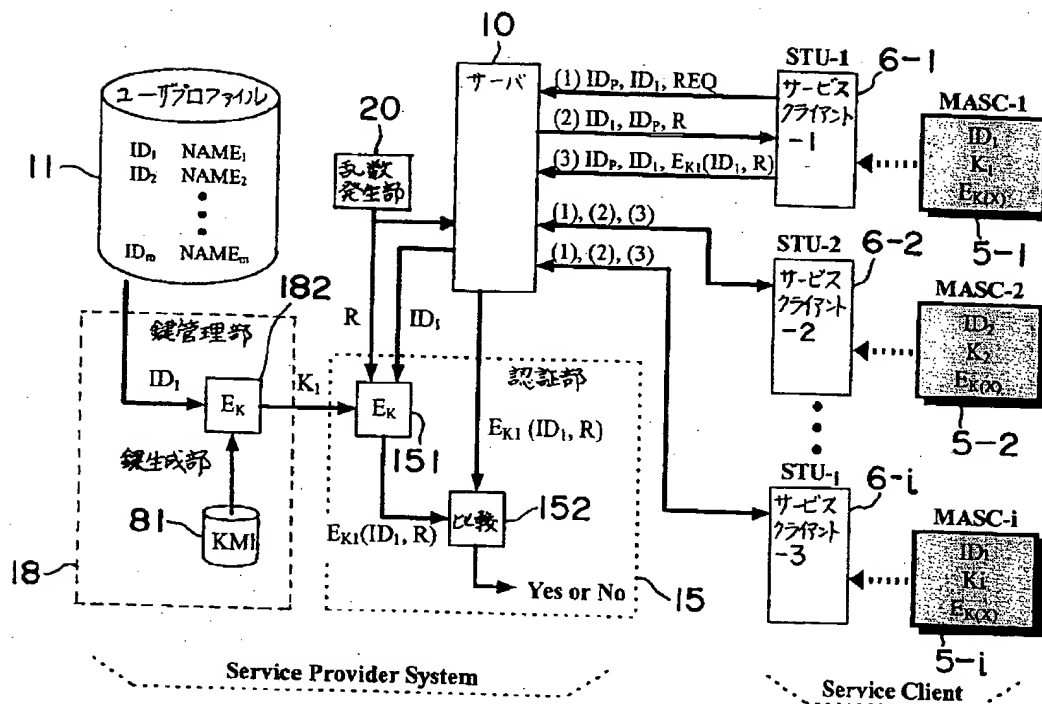


【図4】

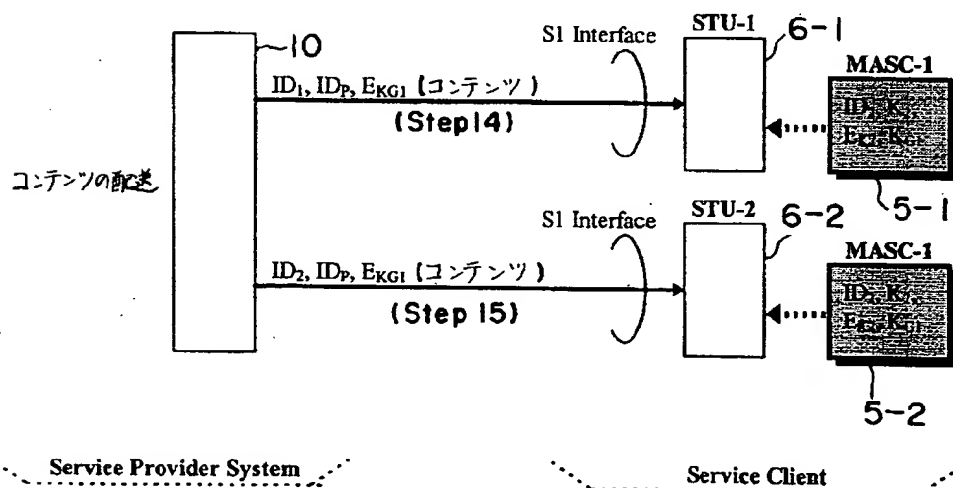
図1のサービスクライアント側システムの構成を示すブロック図



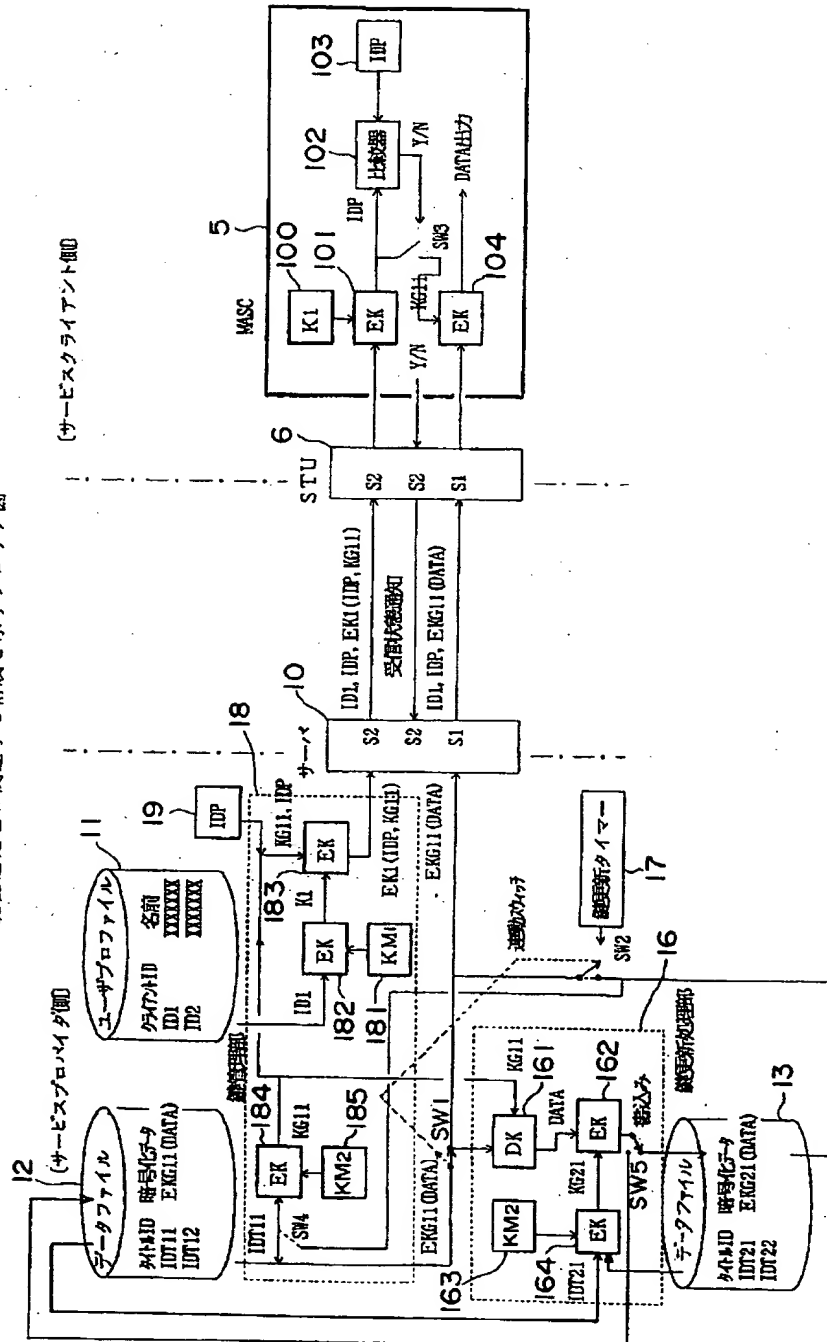
認証処理に関連する構成を示すブロック図



コンテンツ配送処理を示すタイムアロー図

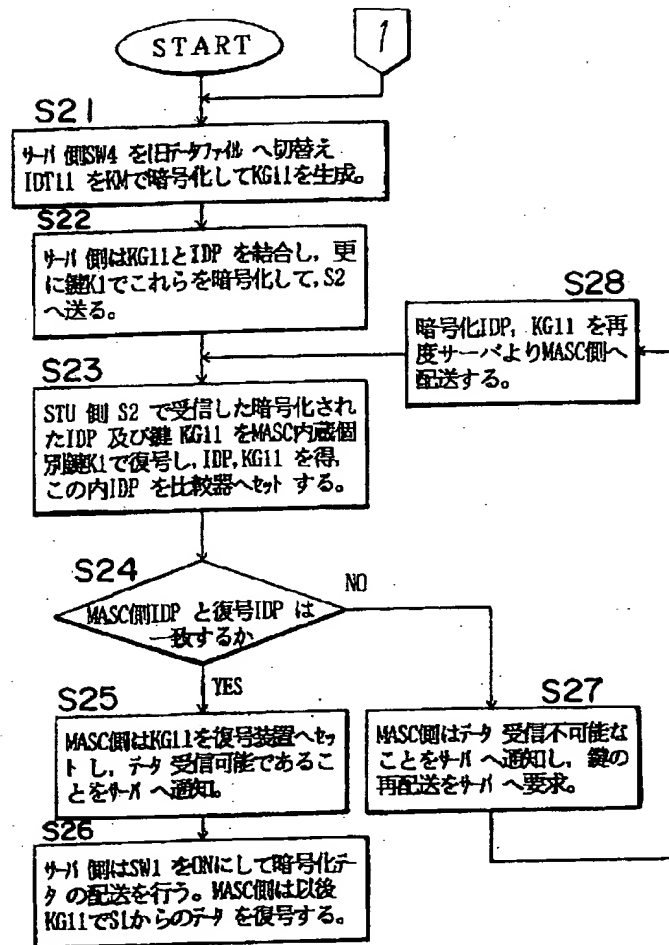


鍵配送処理に関連する構成を示すブロック図



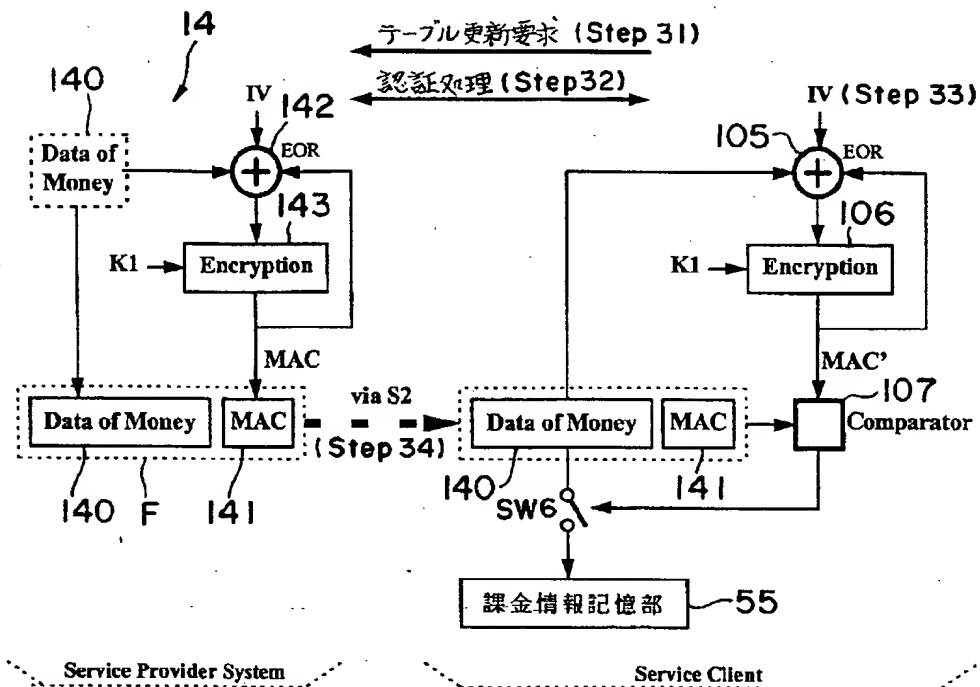
【図10】

鍵配送処理の内容を示すフローチャート



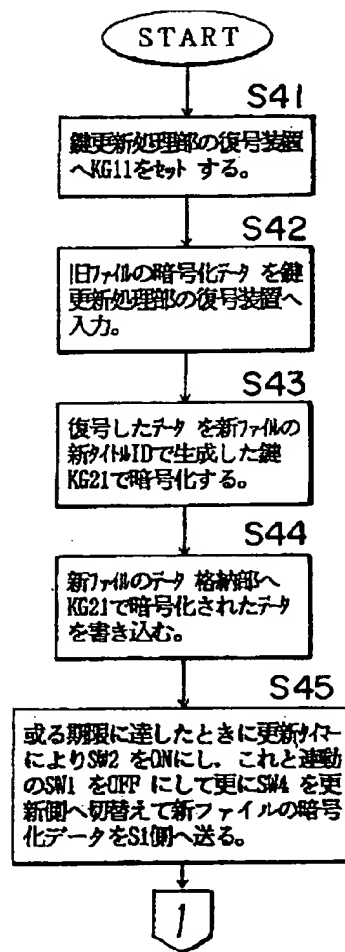
【図13】

デジタル署名処理に関連する構成を示すブロック図



【図14】

鍵の更新処理の内容を示すタイムアロー図



フロントページの続き

(72)発明者 古賀 譲  
 神奈川県川崎市中原区上小田中1015番地  
 富士通株式会社内

(72)発明者 石崎 正之  
 神奈川県川崎市中原区上小田中1015番地  
 富士通株式会社内

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-215242

(43)Date of publication of application : 11.08.1998

(51)Int.Cl. H04L 9/08  
G06F 15/00  
G06F 17/60  
G09C 1/00  
H04L 9/14  
// G06F 12/14

(21)Application number : 09-016085

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 30.01.1997

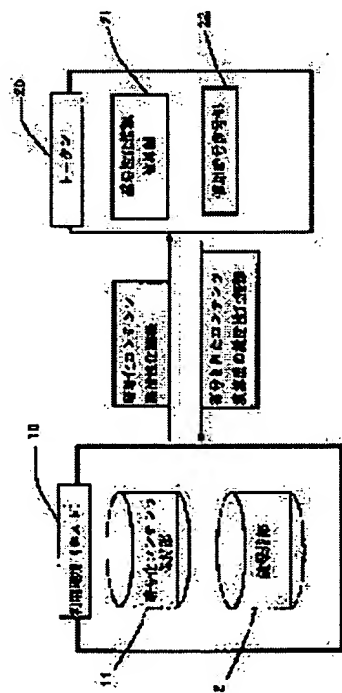
(72)Inventor : KIKO KENICHIROU  
SAITO KAZUO

## (54) AUTHENTICATION METHOD AND DEVICE THEREFOR

### (57)Abstract:

PROBLEM TO BE SOLVED: To execute the control of utilization sequence of enciphered contents in off-line.

SOLUTION: In the case of using a first key, a corresponding key is retrieved from a key storage section 12 based on an ID imparted to contents. A value of a field denoting a remaining number of times corresponding to the key in the key storage section 12 and when the value is zero, a host 10 sends the contents and the key to a token 20. A decoding section 22 of the token 20 uses the key to decode the contents and sends the result to the host 10. The host 10 checks an ID of a key used next to the present key from the key storage section 12. When the ID of the next key is not zero, the host 10 retrieves the next key based on the ID and conducts key activation processing when the corresponding key is found out. When the ID of the next key is zero, since the next key is not in existence, no key activation processing is conducted. The host 10 utilizes the decoded contents.



(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平10-215242

(43)公開日 平成10年(1998)8月11日

(51)Int.Cl. <sup>8</sup>	識別記号	F I	
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z
	17/60	G 0 9 C 1/00	6 6 0 B
G 0 9 C 1/00	6 6 0	G 0 6 F 12/14	3 2 0 B
H 0 4 L 9/14		15/21	Z

審査請求 未請求 請求項の数15 OL (全 22 頁) 最終頁に続く

(21)出願番号 特願平9-16085

(22)出願日 平成9年(1997)1月30日

(71)出願人 000005496

富士ゼロックス株式会社  
東京都港区赤坂二丁目17番22号

(72)発明者 木子 健一郎  
神奈川県足柄上郡中井町境430 グリーン  
テクなかい 富士ゼロックス株式会社内

(72)発明者 齊藤 和雄  
神奈川県足柄上郡中井町境430 グリーン  
テクなかい 富士ゼロックス株式会社内

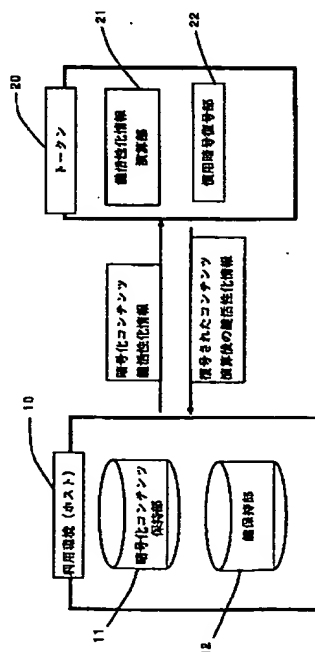
(74)代理人 弁理士 澤田 俊夫

(54)【発明の名称】 認証方法および装置

(57)【要約】

【課題】 暗号化されたコンテンツの利用順序の制御をオフラインで実施できるようにする。

【解決手段】 最初の鍵を使用する際にはコンテンツに付与されたIDを基に対応する鍵を、鍵保持部12より検索する。鍵保持部12の鍵に対応する残り回数のフィールドの値を調べ、値が0の場合にはホスト10はトークン20にコンテンツと鍵を送る。トークン20の復号部22は鍵を利用してコンテンツを復号しホスト10に送る。ホスト10は、鍵保持部12から、現在の鍵の次に使用できる鍵のIDを調べる。次の鍵のIDが0でない場合、IDをもとに次の鍵を検索し、対応する鍵が見つかった場合には、鍵活性化処理を行う。次の鍵のIDが0の場合には、次の鍵は存在しないので、鍵活性化処理は行わない。ホスト10は、復号されたコンテンツを利用する。





## 【特許請求の範囲】

【請求項1】 異なる認証を所定の順序で行う認証方法において、  
先順序の認証のために対応する先順序の証明情報を利用するステップと、

上記先順序の証明情報の利用に基づいて、後順序の認証のための後順序の証明情報を生成するステップと、  
上記後順序の認証のために上記後順序の証明情報を利用するステップとを有することを特徴とする認証方法。

【請求項2】 順序付けて生成された、特定のユーザに対する特定の権利を証明するための証明情報の系列を利用して上記証明情報に対応した認証を行う認証方法において、利用されるべき順序が先である証明情報を利用する際に、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を、生成された証明情報活性化情報に基づいて活性化することによって、証明情報の系列を予め決められた順序でのみ利用できるようにしたことを特徴とする認証方法。

【請求項3】 複数の証明情報から生成された複数の証明情報活性化情報をもとに特定の演算を施す事により、他の証明情報を活性化するための活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行う請求項2記載の認証方法。

【請求項4】 証明情報を利用することで生成される活性化情報を保持しておき、次に同じ証明情報を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く証明情報を活性化することができる証明情報活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行う請求項2記載の認証方法。

【請求項5】 順序付けられた、特定のユーザに対する特定の権利を証明するための証明情報の系列を生成する証明情報生成方法において、利用されるべき順序が先である証明情報から、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を証明情報活性化情報に基づいて改変して生成することによって、先の証明情報を使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしたことを特徴とする証明情報生成方法。

【請求項6】 複数の証明情報から証明情報を活性化するための証明情報活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の証明情報を改変して生成することによって、複数の証明情報を使用することによって、改変した証明情報を有効にするための証明情報活性化情報が得られるようにした請求項5記載の証明情報生成方法。

【請求項7】 利用されるべき順序が先である証明情報から、それに続く証明情報を生成する際に、順序が先で

ある鍵が持つ証明情報活性化情報の初期値に対して複数回の定められた演算を施す事により生成される証明情報活性化情報に基づいて、それに続く証明情報を改変して生成することによって、先の証明情報を複数回使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにした請求項5記載の証明情報生成方法。

【請求項8】 特定のユーザが特定の権利を有することを証明するための証明情報によって、ユーザが正当な権利者であることを認証する装置であって、証明情報を処理して認証を行う際に、それと同時に、当該証明情報に後続して使用されるべき証明情報を使用可能とするための認証情報活性化情報の基となる情報から、後続する証明情報の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する証明情報を利用可能とする証明情報活性化手段を有することを特徴とするユーザ認証装置。

【請求項9】 一連の順序付けられた暗号鍵系列の利用を制御する暗号鍵順序制御方法において、利用されるべき順序が先である鍵を利用する際に、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を、生成された暗号鍵活性化情報に基づいて活性化することによって、暗号鍵系列を予め決められた順序でのみ利用できるようにすることを特徴とする暗号鍵利用順序制御方法。

【請求項10】 複数の鍵から生成された複数の活性化情報をもとに特定の演算を施す事により、他の暗号鍵を活性化するための活性化情報が生成される請求項9記載の暗号鍵利用順序制御方法。

【請求項11】 暗号鍵を利用することで生成される活性化情報を保持しておき、次に同じ暗号鍵を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く暗号鍵を活性化するための暗号鍵活性化情報が生成される請求項9記載の暗号鍵利用順序制御方法。

【請求項12】 一連の順序付けられた暗号鍵系列を生成する暗号鍵生成方法において、利用されるべき順序が先である鍵から、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を暗号鍵活性化情報に基づいて改変して生成することによって、先の鍵を使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしたことを特徴とする暗号鍵生成方法。

【請求項13】 複数の鍵から暗号鍵を活性化するための暗号鍵活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の暗号鍵を改変して生成することによって、複数の鍵を使用することによって、改変した鍵を有効にするための暗号鍵活性化情報が得られるようにした請求項

## 12記載の暗号鍵生成方法。

【請求項14】 利用されるべき順序が先である鍵から、それに続く暗号鍵を生成する際に、順序が先である鍵が持つ暗号鍵活性化情報の初期値に対して複数回の定められた演算を施す事により生成される暗号鍵活性化情報に基づいて、それに続く鍵を改変して生成することによって、先の鍵を複数回使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにした請求項12記載の暗号鍵生成方法。

【請求項15】 暗号化されたデジタル情報を復号して利用するための復号装置であって、復号鍵によって当該暗号化データを復号する際に、それと同時に、当該復号鍵に後続して使用すべき復号鍵を使用可能とするための復号鍵活性化情報の基となる情報を入力として、後続復号鍵の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する復号鍵を利用可能とする復号鍵活性化手段を有することを特徴とした復号装置。

### 【発明の詳細な説明】

#### 【0001】

【発明の属する技術分野】本発明は、複数の認証を所定の順序で行う認証技術に関し、その順序を逸脱した場合には認証が正しく行われないようにしたものである。また本発明は、先の順序の証明情報を利用することにより暗号化されたデジタル情報を復号して利用する場合の、暗号鍵の生成方法に関し、あらかじめ定められた順序に従ってデジタル情報を特定の回数利用することにより、次に定められた暗号鍵が生成される技術に関する。

【0002】なお、本発明の利用範囲はコンテンツを暗号化して流通させ、その利用順序を制御するだけではなく、一般に暗号鍵（署名のための鍵、検証のための鍵など、暗号技術における鍵、一般）の利用順序の制御を可能とするものである。

【0003】従って例えば、電車の乗車券や映画の鑑賞券のようなチケットを電子的に発行する場合に、乗車券はキセルを防ぐために予め決められた順序でしか乗車券を使えないようにしたり、あるいはある映画を見ると別の映画を安く見ることができるなどの鑑賞券の売り方を実現する際にも、電子的に発行されたチケットの利用順序の制御にも適用することが可能である。

#### 【0004】

【従来技術】近年のネットワークの発達により様々な情報がデジタル化され、流通するようになってきている。デジタル情報は複写が容易であり、複写されたものは劣化しないという特質があるため、金銭的な価値を持つデジタルコンテンツ（画像、動画、プログラムなど）を暗号化して流通させ、使用時にユーザの環境で復号して利用するという流通形態が開始され始めている。NTT社のmiTaKaTTa（商標）や、IBM社のInfomarket（商標）が現在実施されている代表的なサ

ービスである。コンテンツが共通の鍵で暗号化されて配布される場合には、一旦鍵が露呈するとその鍵が流布することによってコンテンツがただで利用されてしまうという問題がある。そこで、これらのサービスではコンテンツを利用する時にのみ、オンラインで一時的に鍵を配布し、利用が終わると鍵は捨てられるように構成されている。

【0005】しかし、この構成ではコンテンツの利用がオンラインでしかできないことになり、ユーザに対して通信コストの負担不便を強いることになる。

【0006】一方、それに対して特公平6-95302号公報のソフトウェア管理方式や、WaveSystem社の開発したWaveChip（商標）などの技術では、コンテンツは予め決められた暗号鍵で暗号化されて流通させ、利用者はそれを復号するための共通の鍵の封入されたICカードあるいはICチップを自分のPCに接続し、利用したいときはその装置内で復号してコンテンツを利用するというような形態により構成している。ICカードなどのデバイス内では利用することに履歴が取られ、後でその履歴に応じて料金を徴収するというものであった。

【0007】しかし、この方法によるとユーザの資格などに応じて、利用可能なコンテンツを制限したりすることは不可能であった。

【0008】そこで、本出願人はあらたなユーザ認証技術を提案している（特願平9-418号）。この提案によれば、コンテンツは共通の鍵で暗号化し、ユーザは自分自身の鍵を持ち、アクセスチケットと呼ぶコンテンツとユーザの間を取り持つためのチケットを導入することで、暗号化されたコンテンツのオフラインでの利用を可能とし、さらにユーザ毎にアクセスチケットの発行をコントロールして、アクセス制限を行うことを可能としている。

#### 【0009】

【発明が解決しようとする課題】しかしながら、特願平9-418号の提案によると、コンテンツを利用するためのアクセスチケットはそれを発行可能であるコンテンツの配布者あるいはチケット発行センターのような機関に依頼せねばならない（以下、簡単のためこれらを総称してセンターと呼ぶ）。すなわち、ユーザはアクセスチケットを一旦手に入れてしまえばオフラインで使い続けることが可能となるが、新たなコンテンツを利用しようとした場合には前記センターにオンライン（あるいはそれに代わる手段）で依頼しなければならないことになる。

【0010】予め幾つかの部分に分割され、それらが順序だてて利用されることを想定して作られたコンテンツ、例えば小説や物語、段階を追って難しくすることを意図した問題集などでは、これらのコンテンツは部分に分割され、それぞれの部分ごとに異なった暗号化が施さ

れ、それぞれ利用する際には異なるアクセスチケットを要求するように構成される。

【0011】しかし、コンテンツの利用順序を限定しようとするためには、センターはユーザに対して一括してアクセスチケットを発行することはできないため、ユーザは新たな部分を利用したいと思う度にアクセスチケットを手に入れるためにセンターに発行を依頼しなければならないことになる。

【0012】また、利用順序が線形でなく、二つの異なったコンテンツを順序に関わりなく利用することにより、別のコンテンツが利用可能になるという、提供方法もある。このような販売形態を採ろうとすると、従来の方法では、やはりユーザは三つ目のコンテンツを利用するためのチケットをセンターに発行依頼しなければならない。

【0013】

【発明が解決しようとする課題】本発明は上記のような問題に鑑みてなされたものであり、その目的とするところは、ユーザによる暗号化されたコンテンツ（あるいは暗号鍵）の利用順序の制御をオフラインで実施可能であるようにすることにある。

【0014】

【課題を解決するための手段】まず、本発明の概要について具体的な実現環境に即して説明する。本発明の1実現環境では、上記の課題を解決するため、ユーザ環境をコンテンツの利用環境と、あらかじめユーザ毎に配られるトークンによって構成する。トークンはICカードなどの演算機能を持つ耐タンパー容器である。そして、ある鍵に対して特定の演算を複数回繰り返す事で、始めて次に指定された鍵が生成されるように計算された複数の鍵を発行し、ユーザ環境においてトークンがこの定められた演算を行った結果を基にして、次の鍵を生成することで次の鍵が利用可能になる。

【0015】また、本発明は上記の課題を解決するため、アクセスチケットを用いたアクセス制御方法（特願平9-418号）において、一連の複数のチケットとそれぞれのチケットに対応する利用制限情報をあらかじめ決められた計算方法に基づいて発行する。アクセスチケットの利用制限情報には、このチケットの使用順位もしくは次に使用するチケットを識別する数値、次のチケットを使用可能にするためのチケット活性化情報、次のチケットが使用可能になるまでの回数、及び次のチケットの法数のフィールドが含まれる。そして、発行した複数のチケットと、最初に用いるチケットに対応する利用制限情報のみをユーザに配布する。

【0016】あるチケットの次のチケットを使用可能にするためのチケット活性化情報は、現在使用しているチケットを用いて、トークンとの間で定められた回数の通信を行う事でのみ生成される。こうして生成されたチケット活性化情報を、次に使用するチケットの利用制限情

報の特定のフィールドに追加する事により、はじめて次のチケットが使用可能になる。

【0017】次のチケットは異なるコンテンツに対するものであってもよいし、同一のコンテンツに対して、異なる利用条件での使用を許可するものであってもよい。

【0018】さらに、本発明の構成について詳細に説明する。

【0019】本発明によれば、上述の目的を達成するために、異なる認証を所定の順序で行う認証方法において、先順序の認証のために対応する先順序の証明情報を利用するステップと、上記先順序の証明情報の利用に基づいて、後順序の認証のための後順序の証明情報を生成するステップと、上記後順序の認証のために上記後順序の証明情報を利用するステップとを実行するようにしている。

【0020】この構成においては、先順序の証明情報を実際に使用して初めて後順序の証明情報が利用可能になり、認証を所定の順番で行うように強制できる。

【0021】また、本発明によれば、上述の目的を達成するために、順序付けて生成された、特定のユーザに対する特定の権利を証明するための証明情報の系列の利用して上記証明情報に対応した認証を行う認証法補において、利用されるべき順序が先である証明情報を利用する際に、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を、生成された証明情報活性化情報に基づいて活性化することによって、証明情報の系列を予め決められた順序でのみ利用できるようにしている。

【0022】この構成においては、先の証明情報が利用されて、後の証明情報が活性化されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【0023】また、この構成において、複数の証明情報から生成された複数の証明情報活性化情報をもとに特定の演算を施す事により、他の証明情報を活性化するための活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行うようにしてもよい。

【0024】また、証明情報を利用することで生成される活性化情報を保持しておき、次に同じ証明情報を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く証明情報を活性化することができる証明情報活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行うようにしてもよい。

【0025】また、本発明によれば、上述の目的を達成するために、順序付けられた、特定のユーザに対する特定の権利を証明するための証明情報の系列を生成する証明情報生成方法において、利用されるべき順序が先であ

る証明情報から、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を証明情報活性化情報に基づいて改変して生成することによって、先の証明情報を使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしている。

【0026】この構成においても、先の証明情報が利用されて、後の証明情報が生成されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【0027】また、この構成において、複数の証明情報から証明情報を活性化するための証明情報活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の証明情報を改変して生成することによって、複数の証明情報を使用することによって、改変した証明情報を有効にするための証明情報活性化情報が得られるようにしてもよい。

【0028】また、利用されるべき順序が先である証明情報から、それに続く証明情報を生成する際に、順序が先である鍵が持つ証明情報活性化情報の初期値に対して複数回の定められた演算を施す事により生成される証明情報活性化情報に基づいて、それに続く証明情報を改変して生成することによって、先の証明情報を複数回使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしてもよい。

【0029】また、本発明によれば、上述の目的を達成するために、特定のユーザが特定の権利を有することを証明するための証明情報によって、ユーザが正当な権利者であることを認証する装置において、証明情報を処理して認証を行う際に、それと同時に、当該証明情報に後続して使用されるべき証明情報を使用可能とするための認証情報活性化情報の基となる情報から、後続する証明情報の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する証明情報を利用可能とする証明情報活性化手段とを設けるようにしている。

【0030】この構成においても、先の証明情報が利用されて後の証明情報が活性化されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【0031】また、本発明によれば、上述の目的を達成するために、一連の順序付けられた暗号鍵系列の利用を制御する暗号鍵順序制御方法において、利用されるべき順序が先である鍵を利用する際に、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を、生成された暗号鍵活性化情報に基づいて活性化することによって、暗号鍵系列を予め決められた順序でのみ利用できるようにしている。

【0032】この構成においては、複数の鍵から生成さ

れた複数の活性化情報をもとに特定の演算を施す事により、他の暗号鍵を活性化するための活性化情報が生成されるようにしてもよい。

【0033】また、暗号鍵を利用することで生成される活性化情報を保持しておき、次に同じ暗号鍵を利用する際には、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く暗号鍵を活性化するための暗号鍵活性化情報が生成されるようにしてもよい。

【0034】また、本発明によれば、上述の目的を達成するために、一連の順序付けられた暗号鍵系列を生成する暗号鍵生成方法において、利用されるべき順序が先である鍵から、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を暗号鍵活性化情報に基づいて改変して生成することによって、先の鍵を使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしている。

【0035】この構成においては、複数の鍵から暗号鍵を活性化するための暗号鍵活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の暗号鍵を改変して生成することによって、複数の鍵を使用することによって、改変した鍵を有効にするための暗号鍵活性化情報が得られるようにしてもよい。また、利用されるべき順序が先である鍵から、それに続く暗号鍵を生成する際に、順序が先である鍵が持つ暗号鍵活性化情報の初期値に対して複数回の定められた演算を施す事により生成される暗号鍵活性化情報に基づいて、それに続く鍵を改変して生成することによって、先の鍵を複数回使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしてもよい。

【0036】また、本発明によれば、上述の目的を達成するために、暗号化されたデジタル情報を復号して利用するための復号装置に、復号鍵によって、当該暗号化データを復号する際に、それと同時に、当該復号鍵に後続して使用すべき復号鍵を使用可能とするための復号鍵活性化情報の基となる情報を入力として、後続復号鍵の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する復号鍵を利用可能とする復号鍵活性化手段とを設けるようにしている。

【0037】この構成においては、先行する復号鍵を利用することにより後続の復号鍵を活性化させることで可能となり、予め定められた順序で復号を行うことが可能となる。

【0038】

【発明の実施の態様】以下、本発明の実施例について説明する。

【0039】【実施例1】本実施例では、1つの暗号化

鍵を特定の回数用いる事により、異なるコンテンツに対する暗号化鍵を生成する方法について述べる。

【0040】本実施例は、デジタルコンテンツを暗号化して鍵と共に提供するコンテンツプロバイダと、提供されたコンテンツを復号して利用するためのユーザ環境とからなる。

【0041】図1は、ユーザ環境を示しており、この図において、ユーザ環境は、利用環境（ホスト）10とトークン20とからなり、利用環境10は暗号化されたデジタルコンテンツを保持するコンテンツ保持部11と、それに対応する鍵を保持する鍵保持部12とを含んで構成されている。トークン20はあらかじめユーザ毎に配布される、スマートカードやICカードであり、鍵を活性化させるための演算部21とコンテンツ、もしくはコンテンツを復号するための情報を復号するための復号部22を持つ。

【0042】次に実施例の動作について図2および図3を参照して述べる。図2は実施例の全体的な処理を示す。図3は鍵活性化処理の詳細を示す。

【0043】なお、本実施例では、コンテンツプロバイダは4つの異なるコンテンツが順番に利用されるように、鍵を発行する。始めにコンテンツプロバイダは、コンテンツを慣用暗号鍵K1で暗号化する。さらに、他のコンテンツを、利用する順番にそれぞれK2～K4の鍵で暗号化する。そして、以下のように、 $K2' \sim K4'$ を計算する。

【0044】

【数1】 $K2' = K2 - FUr2(K1)$

$K3' = K3 - FUr3(K2)$

$K4' = K4 - FUr4(K3)$

$FUr2(K1)$ はK1に対してFの演算をUr2回繰り返す事を意味している。

【0045】Fは一方方向性関数（例えばMD5などのハッシュ関数）、Urは次のチケットを使用可能にするために現在のチケットを使用しなければならない回数である。Fの計算方法を秘密とし、ユーザ毎にその計算方法を異なるものとすれば、他のユーザが計算した値を流用される事はない。ユーザには、K1と $K2' \sim K4'$ および、 $Ur2 \sim Ur4$ が配布される。ユーザに配布された鍵は鍵保持部12に保持される。一連の鍵が配布された時点での、鍵保持部12の様子を図4に示す。

【0046】さて、図2において、最初の鍵を使用する際にはコンテンツに付与されたIDを基に対応する鍵を、鍵保持部12より検索する（S10）。対応する鍵が無い場合は処理を終了する（S11）。次に、鍵保持部12の鍵に対応する残り回数のフィールドの値を調べ、値が0でない場合はその鍵はまだ有効ではないので、やはり処理を終了する（S12）。ホスト10はトークン20にコンテンツと鍵を送る（S13）。トークン20の復号部22は鍵を利用してコンテンツを復号し

ホスト10に送る（S14）。ホスト10は、鍵保持部12から、現在の鍵の次に使用できる鍵のIDを調べる（S15）。次の鍵のIDが0でない場合、IDをもとに次の鍵を検索し、対応する鍵が見つかった場合には、鍵活性化処理を行う（S16～S19）。次の鍵のIDが0の場合には、次の鍵は存在しないので、ホスト10は復号されたコンテンツを利用する（S20）。

【0047】次に図3を参照して鍵活性化処理S19について詳細に述べる。図3において、鍵活性化処理では、まず鍵保持部12から鍵に対応する鍵活性化情報を取得する（S21）。この値が0であった場合には、鍵活性化情報のフィールドに、現在の鍵の値を書き込む（S22、S23）。次に、ホスト10はトークン20に現在の鍵活性化情報aを送る（S24）。トークン20は $F(a)$ を計算しホスト10にその値を返す（S25）。鍵保持部12の、次の鍵の残り回数Urの値（図4）を1減らす（S26）。1減らした結果、残り回数Urの値が0にならない場合には、ユーザ環境はF

(a)の値で、現在の鍵の活性化情報を置き換える（S27、S28）。値が0になった場合には、次の鍵の値に $F(a)$ を足したもので、次の鍵の値を置き換える（S29）。このようにして2番目の鍵が使用可能になった時点での、鍵保持部12の様子を図5に示す。これで、鍵活性化処理は終了し、ホスト10は復号されたコンテンツを利用する。

【0048】このように一連の鍵を上記のような方法で、関連付けて作成する事により、第一の鍵K1を特定回数使うことにより、初めて、第二の鍵K2を計算する事ができ、これにより第二の鍵K2が利用可能になる。同様の処理により、順次異なる鍵を、定まった順序・回数でのみ利用する仕組みが実現できる。

【0049】【実施例2】本実施例では、特に1つのコンテンツを特定の回数用いる事により、異なる利用条件での使用を可能にする方法について述べる。例えば、あるコンテンツを特定回数用いることで、より安い料金での使用を可能にするような方法である。

【0050】また、本実施例は、本発明を特願平9-418号のユーザ認証技術に適用した例である。

【0051】はじめに、本実施例で用いられるアクセスチケット（認証用補助情報）を用いた処理の概観を説明する。図6に処理の概観を示す。図6において、アクセスチケットを用いた処理は、チケット発行センタ30と、コンテンツプロバイダ40、及びユーザ環境50から構成されるシステムにおいて実行される。

【0052】チケット発行センタ30は、チケット公開鍵データベース31、ユーザデータベース32、プロバイダデータベース33及びアクセスチケット発行装置34を持つ。コンテンツプロバイダ40は、暗号化していないコンテンツと、慣用暗号鍵を保持し、慣用暗号装置よりコンテンツを暗号化する。

【0053】また、ユーザ環境50は、パソコンやワークステーションなど、デジタル情報を利用するための情報処理装置である利用環境（ホスト）51と、利用者の認証をするためにホスト51に接続されているトークン52とを含んでなる。ホスト51はユーザツール53およびカプセル化コンテンツ54を含む。トークン52は、各利用者に固有の情報を安全に封入したICカードもしくはスマートカードのような耐タンパー容器であり、固有情報をもとに利用者の認証を行うための演算部を有している。トークン52はあらかじめ各利用者に配布されている。

【0054】はじめに、コンテンツプロバイダ40は、コンテンツを暗号化する慣用暗号鍵を暗号化するために必要なRSA（Rivest, Shamir, Adleman）公開鍵の発行を、チケット発行センタ30に対して要求する(①)。チケット発行センタ30は要求に応じて、公開鍵をコンテンツプロバイダ40に送付する(②)。コンテンツプロバイダ40は自身で用意した慣用暗号鍵でコンテンツを暗号化し、その鍵をさらに発行された公開鍵で暗号化してコンテンツ内に特定の方法で埋め込む。こうして出来上がったコンテンツ（カプセル化コンテンツ）が、利用者（ユーザ環境）50にネットワークやCD-ROMなどを用いて配布される(③)。コンテンツは暗号化されているため、このままでは利用する事ができない。利用者は利用したいコンテンツ及び自分のユーザIDに対応したアクセスチケットの発行をセンタ30に要求する(④)。アクセスチケットは、特定のコンテンツとユーザの固有情報がそろったときのみ、そのコンテンツを利用可能にするためのデジタル情報であり、他のユーザとコンテンツの組み合わせでは使用できない。センタ30はユーザの要求に応じてアクセスチケットを発行しユーザに送付する(⑤)。ユーザはアクセスチケットを用いてコンテンツを利用する。アクセスチケットにはアクセス制御のための情報以外に、利用料金や支払方法、使用期限などの利用条件に関する情報が付与されている。ユーザがコンテンツを利用すると、利用に応じてその履歴がトークン52に記録される。この際、履歴にはその利用時点での利用条件も同時に記録される。ユーザは適当なタイミングで、センタ30に利用履歴を送付する(⑥)。センタ30は回収した利用履歴に基づいて課金を行う。回収した履歴に基づいて計算された料金が、それぞれの利用者の口座より引き落とされ、コンテンツプロバイダ40に各コンテンツの利用量に応じて分配される(⑦)。

【0055】次に、本実施例での処理を詳しく説明する。

【0056】はじめに、コンテンツプロバイダ40は、コンテンツを暗号化する慣用暗号鍵を暗号化するために必要なRSA公開鍵ペアE、Dと法数nをセンタ30より発行してもらう。コンテンツプロバイダ40にはEと

nが渡され、センタ30は発行した公開鍵に対応する秘密鍵D、法数nを公開鍵データベース31に記録して安全に管理しておく。次に、コンテンツプロバイダ30は自身で用意した慣用暗号鍵Kによりこのコンテンツを暗号化する。さらに、このKをセンタより発行された公開鍵Eで暗号化し、 $K^* = K^E \bmod n$ を作成する。この $K^*$ をコンテンツ内に特定の方法で埋め込む。こうして出来上がったコンテンツ（以下カプセル化コンテンツと呼ぶ）は、利用者にネットワークやCD-ROMなどを用いて配布される。

【0057】ユーザはコンテンツを利用するため、アクセスチケットの発行をセンタ30に依頼する。図7にアクセスチケットの構成を示す。アクセスチケットは認証情報（以下単にチケットと呼ぶ）tと、利用制限情報L、チケット法数n、及び公開鍵Eからなる。アクセスチケットとコンテンツは一意に対応しており、コンテンツの公開鍵法数nによって対応関係を決定することができる。

【0058】ここで、ある一定回数利用後には異なった利用条件（例えば割引料金）での使用を可能にするため、アクセスチケットを発行する際に、センタ30は以下のように、複数のチケットとそれに対応する利用制限情報を用意する。本実施例では4種類の異なる利用条件を持つアクセスチケットとそれに対応する利用制限情報を用意する。

【0059】

【数2】 $t_1 = D + F(du, L_1, n)$

$t_2 = D + F(du, L_2, n)$

$t_3 = D + F(du, L_3, n)$

$t_4 = D + F(du, L_4, n)$

利用制限情報を図8に示す。

【0060】上記の式および図8において、式「 $(a_1) F_{ur2}(du, L_1, n) \bmod n$ 」は、 $a_1$ を $F(du, L_1, n)$ でUr2回べき乗し、nに関する剰余をとることを表す。tはチケット、Dはコンテンツの公開鍵に対応する秘密鍵、Fは一方方向性関数（例えばMD5などのハッシュ関数）、duはユーザの秘密鍵、nはコンテンツの公開鍵法数、lrはチケット発行時に生成される乱数、Lは利用条件などを記した利用制限情報である。

【0061】利用制限情報Lは、対応するチケットによるコンテンツの利用に関する情報を記述したもので、アクセスチケットが利用できる期限を示す使用期限や、このチケットによってコンテンツを利用した場合の1回の利用料金などが記述されている。コンテンツを利用した場合には、この情報に従って課金が行われる。さらに、利用制限情報Lには、このアクセスチケットの使用順位、次のアクセスチケットを使用可能にするためのチケット活性化情報a、及び次のアクセスチケットが使用可能になるまでの回数Urが含まれている。

【0062】チケット生成時には、 $t$ は $L$ を図8に示すように設定して計算される。すなわち、 $U_r$ の値を全て0とし、 $\alpha$ の計算にのみ実際の $U_r$ の値が用いられる。 $n$ 、 $D$ の値はセンタ30内の公開鍵データベース31を、 $du$ の値はユーザデータベース32を参照する事により得ることができる。

【0063】ユーザには $t_1$ から $t_4$ の一連のチケットと、利用制限情報 $L_1 \sim L_4$ を含むアクセスチケットが配布される。但し、ユーザへの配布時には $L_1 \sim L_4$ は、図9に示すように $U_{r1} \sim U_{r4}$ に値が設定され、さらに $L_2 \sim L_4$ の $\alpha_2 \sim \alpha_4$ の値を0としたものに置き換えられる。

【0064】図10にユーザ環境50(図6)の構成を示す。ユーザ環境50は利用環境(ホスト)51とトークン52からなり、トークン52は証明情報演算部64およびユーザ固有情報保持部65を有している。ユーザ固有情報保持部65には各ユーザに固有の情報が入れられている。固有情報はユーザには秘密であり、ユーザのIDとそれに対応する固有情報は、チケット発行センタ30で安全に管理されている。

【0065】利用環境(ホスト)51は、カプセル化コンテンツ54とユーザツール53とを有する。ユーザツール53は、アクセスチケット保持部(複数のチケット)55、アクセスチケット検索部56、および証明情報演算部57を持つ。また、カプセル化コンテンツ54には、乱数発生部58、チケット公開鍵法数保持部59、チケット公開鍵保持部60、慣用暗号復号部61、暗号化された慣用鍵の保持部62、および暗号化コンテンツ保持部63を有する。

【0066】次に、ユーザ環境50での処理について述べる。図11および図12にユーザ環境50での処理を示す。ユーザ環境では以下の処理を行う。

【ステップS31】カプセル化コンテンツ54が乱数 $r$ を生成する。

【ステップS32】カプセル化コンテンツ54が $r^{EK} \bmod n$ を計算し、この値とコンテンツの公開鍵法数 $n$ とをユーザツール53に送付する。 $r$ を用いるのはトークンとの通信路上で慣用暗号鍵を知られるのを防ぐためである。

【ステップS33】ユーザツール53が、管理しているチケット保持部55から、 $n$ を法数として持つアクセスチケットを全て検索する。チケット保持部55は、法数 $n$ と対応するチケットを組にして保持している。

【ステップS34】アクセスチケットが1つも見つからない場合は、処理を終了する。

【ステップS35】検索したチケットの中から、利用制限情報の残り使用回数 $U_r$ が0のチケットで、最も使用順位の値が大きいものを選択する。

【ステップS36】現在のチケットと同じ法数 $n$ を持つチケットの中から、現在のチケットの次に使用順位の

値が大きいチケットを検索する。

【ステップS37、S38、S39】チケットが見つかった場合、そのチケットの活性化情報の値を調べ、その値が0の場合には現在のチケットの活性化情報の値を書き込む。そして、 $r^{EK} \bmod n$ 、法数 $n$ 、現在のチケットの利用制限情報 $L$ 、及び次のチケットの活性化情報 $\alpha$ の値をトークン52に送る。活性化情報がゼロでない場合はそのまま $r^{EK} \bmod n$ 、法数 $n$ 、現在のチケットの利用制限情報 $L$ 、及び次のチケットの活性化情報 $\alpha$ の値をトークン52に送る。

【ステップS36、S40】チケットが見つからない場合、 $\alpha$ の値を0として、 $r^{EK} \bmod n$ 、 $n$ 、 $L$ 、 $\alpha$ の組みをトークン52に送る。

【ステップS41】トークン52が、

【0067】

$$[数3] R1 = (r^{EK})^F(du, L, n)$$

$$R2 = (\alpha)^F(du, L, n)$$

を計算する。

【ステップS42】ユーザツール53は、トークン52が計算を行っている間に、 $(r^{EK})^t$ の値を計算する。

【ステップS43】トークン52は、計算した $R1$ 、 $R2$ の値をユーザツール53に送る。

【ステップS44~S46】次の使用順位のチケットがある場合には、ユーザツール53は次のチケットの利用制限情報中の残り回数 $U_r$ の値を1減らし、さらに、次のチケットの活性化情報フィールドの値を、 $R2$ の値で置き換える。

【ステップS47】トークン52から受け取った $R1$ から、

$$(r^{EK})^t \cdot R1^{-1} = r^K \bmod n$$

を計算してカプセル化コンテンツ54に送付。

【ステップS48】カプセル化コンテンツ54は、 $r^K$ より $K$ を求める。 $r$ の値はカプセル化コンテンツ49が発生させたものなので、 $K$ の計算が可能である。

【ステップS49】カプセル化コンテンツ54は、 $K$ により暗号化されたコンテンツ本体を慣用暗号復号部61により復号して利用する。

【0068】最初のチケット $t_1$ を1回使用した時点での、利用制限情報は図13に示すようになる。

【0069】ユーザがコンテンツを利用すると、その利用時点での利用条件がトークン52に履歴として記録される。同じコンテンツであっても利用時点での利用条件での履歴が記録されるため、定まった利用順序・回数で定まった利用条件によるコンテンツの利用が可能になる。

【0070】このようにチケットと利用制限情報の組を計算しておくことにより、例えば、第一のチケット $t_1$ を特定回数使うことで始めて、 $t_2$ の計算に用いられた $L_2$ 中の $\alpha_2$ を計算する事ができ、第二のチケットが利



用可能になる。第2のチケットの利用条件を第1のチケットと異なるものとする事で、例えば利用料金の割引などを行う事が可能になる。同様の処理により、順次異なった条件のチケットを、定まった順序・回数で利用する仕組みが実現できる。

【0071】【実施例3】本実施例では特に、1つのコンテンツを特定の回数利用する事により、それとは異なったコンテンツの使用を定められた順番で可能にする方法について述べる。

【0072】本実施例では実施例2と同様にアクセスチケットによる処理を行う。

【0073】本実施例の構成は実施例2と同様であるが、アクセスチケットの利用制限情報に、使用順位の代わりに、次に使用可能となるコンテンツに対応する法数を入れるフィールドが追加される点異なる。

【0074】実施例の動作について説明する。

【0075】実施例2と同様の方法により、コンテンツプロバイダ40はセンタ30から発行してもらった公開鍵を用いてコンテンツをカプセル化して配布する。ユーザは同様に、センタ30に対してアクセスチケットの発行を要求する。

【0076】ここで、あるコンテンツを特定回数利用した場合のみ、それとは異なるコンテンツを定まった順番で利用できるようにするため、アクセスチケットを発行する際に、センタは以下のように、複数のチケットとそれに対応する利用制限情報を用意する。本実施例では4種類の異なるコンテンツと、それぞれのコンテンツに対応するアクセスチケットとそれに対応する利用制限情報(図14)を用意する。

【0077】アクセスチケットは次式のようなものである。

【0078】

【数4】  $t1 = D1 + F(du, L1, n1)$

$t2 = D2 + F(du, L2, n2)$

$t3 = D3 + F(du, L3, n3)$

$t4 = D4 + F(du, L4, n4)$

利用制限情報は図14に示すようなものである。

【0079】上記の式および図14において式「 $(a1) \text{Fur2}(du, L1, n2) \bmod n$ 」は、 $a1$ を $F(du, L1, n2)$ で $Ur2$ 回べき乗し、 $n$ に関する剰余をとることを表す。 $t$ はチケット、 $D$ はコンテンツの公開鍵に対応する秘密鍵、 $F$ は一方方向性関数(例えばMD5などのハッシュ関数)、 $du$ はユーザの秘密鍵、 $n$ はコンテンツの公開鍵法数、 $lr$ はチケット発行時に生成される乱数、 $L$ は利用条件などを記した利用制限情報である。

【0080】利用制限情報 $L$ は、対応するチケットによるコンテンツの利用に関する情報を記述したもので、アクセスチケットが利用できる期限を示す使用期限や、このチケットによってコンテンツを利用した場合の1回の

利用料金などが記述されている。コンテンツを利用した場合には、この情報に従って課金が行われる。さらに、利用制限情報 $L$ には、次のアクセスチケットを使用可能にするためのチケット活性化情報 $a$ 、次のアクセスチケットが使用可能になるまでの回数 $Ur$ 、および次に使用可能になるチケットの法数が含まれている。

【0081】チケット生成時には、 $t$ は $L$ を上記の表のように設定して計算される。すなわち、 $Ur$ の値を全て0とし、 $a$ の計算にのみ実際の $Ur$ の値が用いられる。

【0082】ユーザには $t1$ から $t4$ の一連のチケットと、利用制限情報 $L1 \sim L4$ を含むアクセスチケットが配布される。但し、ユーザへの配布時には $L1 \sim L4$ は、図15に示すように $Ur1 \sim Ur4$ に値が設定され、さらに $L2 \sim L4$ の $a2 \sim a4$ の値を0としたものに置き換えられる。

【0083】次に、ユーザ環境での処理について述べる。ユーザ環境50の構成は実施例2と同様である。図16および図17にユーザ環境50での処理を示す。ユーザ環境50では以下の処理を行う。

【ステップS51】 カプセル化コンテンツ54が乱数 $r$ を生成する。

【ステップS52】 カプセル化コンテンツ54は $rE \text{KE} \bmod n$ を計算し、この値とコンテンツの公開鍵法数 $n$ をユーザツール53に送付する。 $r$ を用いるのはトークン52との通信路上で慣用暗号鍵を知られるのを防ぐためである。

【ステップS53】 ユーザツール53は、管理しているチケット保持部55から、 $n$ を法数として持つチケットを検索する。チケット保持部55は、法数 $n$ と対応するチケットを組にして保持している。

【ステップS54】 チケットが見つからなかった場合は処理を終了する。

【ステップS55】 検索したチケットの残り利用回数 $Ur$ が0でなければ、そのチケットはまだ有効ではないので、処理を終了する。

【ステップS56】 ユーザツール53は現在のチケットの利用制限情報 $L$ の、次のチケットの法数の値を調べ

【ステップS57～S60】 法数の値が0ではなく、この法数に対応する次のチケットが存在する場合、そのチケットの活性化情報の値を調べ、その値が0の場合には現在のチケットの活性化情報の値を書き込む。

【ステップS61】 さらに $rE \text{KE} \bmod n$ 、法数 $n$ 、現在のチケットの利用制限情報 $L$ 、及び次のチケットの活性化情報 $a$ の値をトークン52に送る。

【ステップS62】 次のチケットの法数の値が0か、法数の示すチケットが存在しない場合には、 $a$ の値を0をとって、 $rE \text{KE} \bmod n$ 、 $n$ 、 $L$ 、 $a$ の組みをトークン52に送る。

【ステップS63】 トークン52は



【0084】

【数5】  $R1 = (r^{EKE}) F(du, L, n)$ 、  
 $R2 = (\alpha) F(du, L, n)$

を計算する。

【ステップS64】 ユーザツール53はトークン52が計算を行っている間に、 $(r^{EKE}) t$ の値を計算する。

【ステップS65】 トークン52は、計算したR1、R2の値をユーザツール53に送る。

【ステップS66～S68】 次のチケットがある場合には、ユーザツール53は、次のチケットの利用制限情報中の残り回数U<sub>r</sub>の値を1減らし、さらに、次のチケットの活性化情報フィールドの値を、R2の値で置き換える。

【ステップS69】 トークン52から受け取ったR1から、

【0085】

【数6】  $(r^{EKE}) t \cdot R1^{-1} = r^K \bmod n$ を計算してカプセル化コンテンツ54に送付する。

【ステップS70】 カプセル化コンテンツ54は、 $r^K$ よりKを求める。 $r$ の値はカプセル化コンテンツ54が発生させたものなので、Kの計算が可能である。

【ステップS71】 カプセル化コンテンツ54は、Kにより暗号化されたコンテンツ本体を慣用暗号復号部61により復号して利用する。

【0086】最初のチケットt1を1回使用した時点での、利用制限情報は図18に示すようになる。

【0087】実施例2と同様の方法により、ユーザの利用に応じて利用履歴がトークン52に記録され、これをセンタ30が回収する事により、利用者への課金とコンテンツプロバイダ40への料金の分配が行われる。

【0088】このようにチケットと利用制限情報の組をあらかじめ計算して配布することにより、例えば、第一のチケットt1を特定回数使うことで始めて、t2の計算に用いられたL2中の $\alpha 2$ を計算する事ができ、第二のチケットが利用可能になる。第2のチケットには異なるコンテンツが対応づけられており、これにより、定まった順序で次のコンテンツを使用させる事ができる。同様の処理により、順次異なったコンテンツを、あらかじめ定められた順序でのみ利用させる仕組みが実現できる。

【0089】また、本実施例の変形として、2つのアクセスチケットを1回ずつ利用する事で、はじめて他のチケットを使用可能にするような仕組みも実現可能である。そのために、センタは以下のようなチケットと利用制限情報を用意する。

【0090】アクセスチケットは次のようなものである。

【0091】

【数7】  $t1 = D1 + F(du, L1, n1)$

$t2 = D2 + F(du, L2, n2)$

$t3 = D3 + F(du, L3, n3)$

利用制限情報は図19に示すようなものである。

【0092】上記の式および図19において、 $lr1$ 、 $lr2$ はチケット発行時に生成される乱数、Nはこのチケットを活性化させるのに必要な活性化情報の数である。また、fは使用履歴を示すフラグで、1度使われるとこの値は1に書き換えられる。

【0093】ユーザにはt1からt3の一連のチケットと、利用制限情報L1～L3を含むアクセスチケットが配布される。但し、ユーザへの配布時には図20に示すように、L3は、 $\alpha 3$ の値を0としたものに置き換えられる。

【0094】t1、t2を最初に使用すると、それぞれの使用履歴が1に書き換えられるとともに、t3のための活性化情報

【0095】

【数8】  $\alpha 1' = \alpha 1 F(du, L1, n1)$

$\alpha 2' = \alpha 2 F(du, L2, n2)$

が計算されて、L3に保持される。t3を使用する際に、N3個の必要な活性化情報がそろっていた場合には、

【0096】

【数9】  $\alpha 3 = \alpha 1' + \alpha 2' = \alpha 1 F(du, L1, n1) + \alpha 2 F(du, L2, n2)$

が計算できるので、t3の使用が可能になる。

【0097】このようにすることで、t1、t2の利用の順番を特定せずに、両方のチケットを使ったときのみ、t3が有効になる仕組みを実現できる。

【0098】

【発明の効果】以上のように、本発明を用いる事で、オフライン環境下においても、ユーザ環境および提供するコンテンツそのものに特段の機構を追加することなく、また、センタとのコンテンツの利用毎の通信を伴うこともなしに、暗号化されたコンテンツ（あるいは暗号鍵）の利用順序の制御が可能になる。

【図面の簡単な説明】

【図1】 本発明の実施例1の構成を示すブロック図である。

【図2】 実施例1の処理を説明するフローチャートである。

【図3】 実施例1の処理を説明するフローチャートである。

【図4】 実施例1の鍵保持部の構造（初期値）を示す図である。

【図5】 実施例1の鍵保持部の構造（2番目の鍵K2が使用可能になった状態）を示す図である。

【図6】 本発明の実施例2で用いるアクセスチケットによる処理を説明する図である。

【図7】 アクセスチケットの構成を示す図である。

【図8】 実施例2の利用制限情報を説明する図である。

【図9】 実施例2の利用制限情報（ユーザに当初送られるもの）を説明する図である

【図10】 実施例2のユーザ環境の構成を示すブロック図である。

【図11】 実施例2の動作を説明するためのフローチャートである。

【図12】 実施例2の動作を説明するためのフローチャートである。

【図13】 実施例2の利用制限情報（最初のチケットを1回利用した後のもの）を説明する図である。

【図14】 本発明の実施例3の利用制限情報を説明する図である。

【図15】 実施例3の利用制限情報（ユーザに当初送られるもの）を説明する図である。

【図16】 実施例3の動作を説明するフローチャート

である。

【図17】 実施例3の動作を説明するフローチャートである。

【図18】 実施例3の利用制限情報（最初のチケットを1回利用した後のもの）を説明する図である。

【図19】 実施例3の変形例の利用制限情報を説明する図である。

【図20】 上述変形例の利用制限情報（ユーザに当初送られるもの）を説明する図である。

【符号の説明】

- 10 利用環境（ホスト）
- 11 暗号化コンテンツ保持部
- 12 鍵保持部
- 20 トークン
- 21 鍵活性化情報演算部
- 22 慣用暗号復号部22

【図4】

鍵ID	鍵	次の鍵ID	鍵活性化情報	使用可能になるまでの回数
$I_1$	$K_1$	$I_2$	0	0
$I_2$	$K_2$	$I_3$	0	$Ur2$
$I_3$	$K_3$	$I_4$	0	$Ur3$
$I_4$	$K_4$	0	0	$Ur4$

【図5】

鍵ID	鍵	次の鍵ID	鍵活性化情報	使用可能になるまでの回数
$I_1$	$K_1$	$I_2$	$\sigma_1 = F^{Ur1-1}(a_1)$	0
$I_2$	$K_2 = K_1 + F(a_1)$	$I_3$	0	0
$I_3$	$K_3$	$I_4$	0	$Ur3$
$I_4$	$K_4$	0	0	$Ur4$

【図7】

アクセスチケット
チケット法数 $n$
公開鍵 $E$
チケット本体 $t$
利用制限情報 $L$

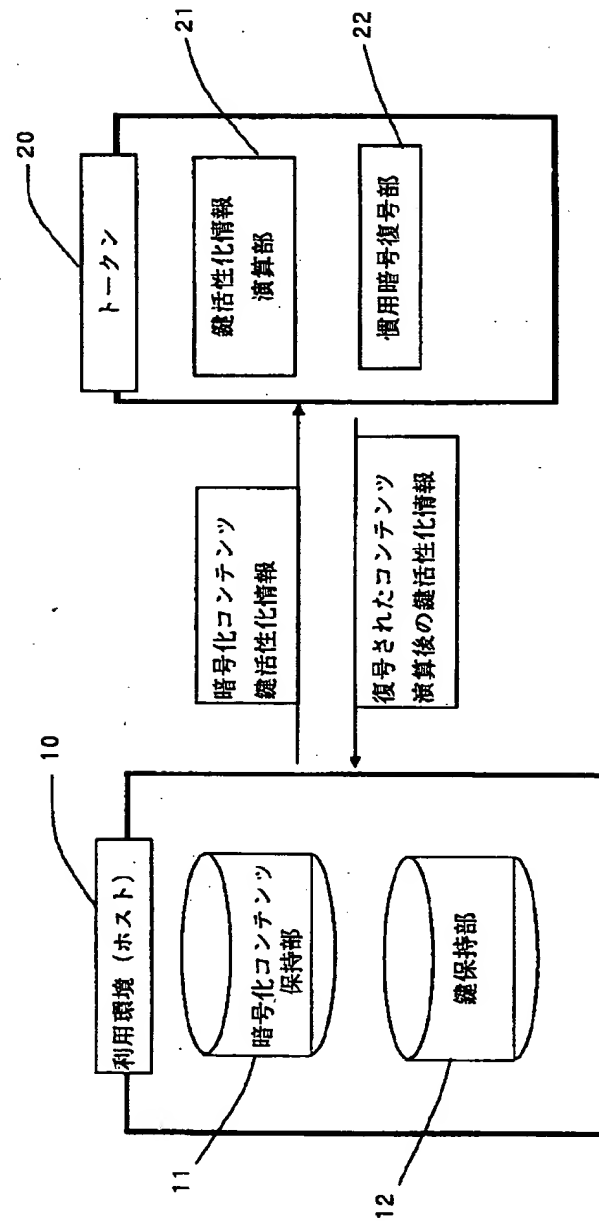
【図9】

利用制限情報	使用期限	利用料金	使用順位	使用可能になるまでの回数	チケット活性化情報
$L_1$	1997/12/31	100	1	$Ur1=0$	$\sigma_1 = Ir$
$L_2$	1997/12/31	80	2	$Ur2=20$	$\sigma_2 = 0$
$L_3$	1997/12/31	60	3	$Ur3=20$	$\sigma_3 = 0$
$L_4$	1997/12/31	40	4	$Ur4=20$	$\sigma_4 = 0$

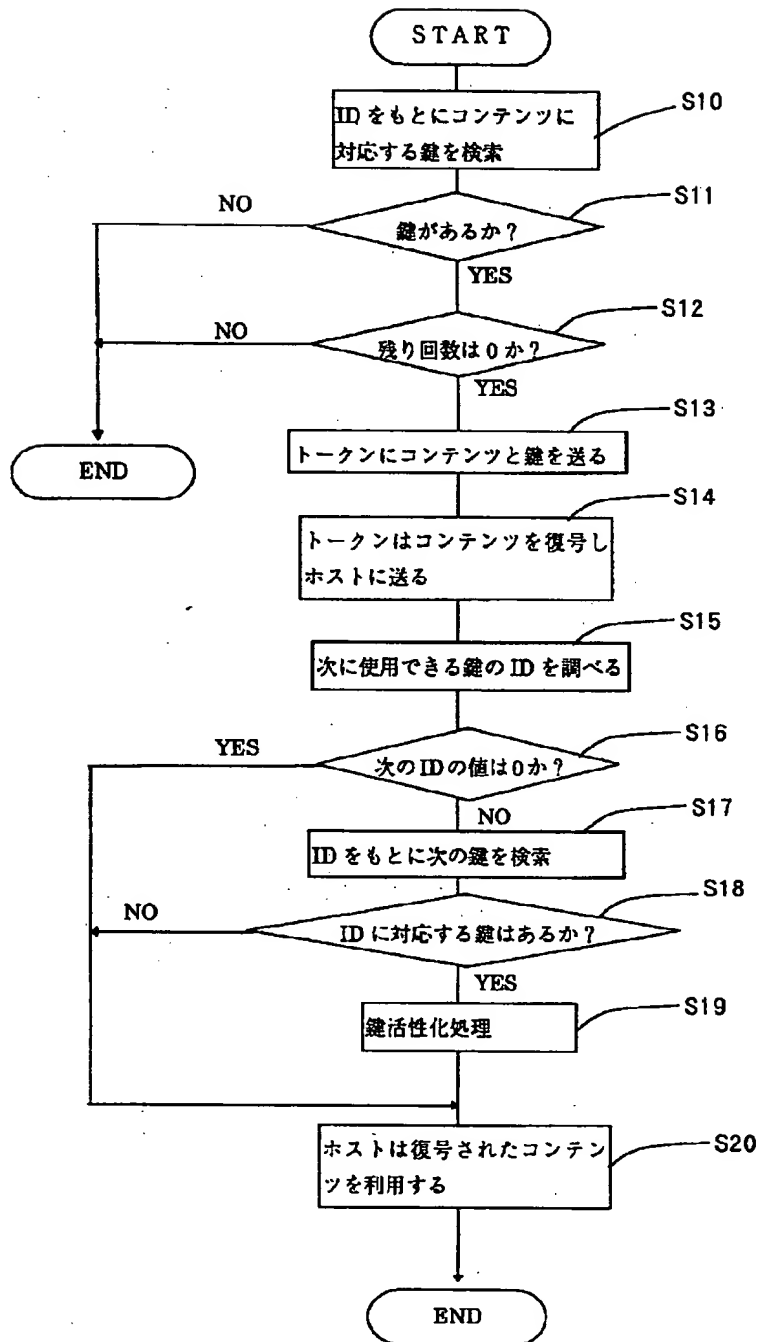
【図13】

利用制限情報	使用期限	利用料金	使用順位	使用可能になるまでの回数	チケット活性化情報
$L_1$	1997/12/31	100	1	$Ur1=0$	$\sigma_1 = Ir$
$L_2$	1997/12/31	80	2	$Ur2=19$	$\sigma_2 = (a_1^{Ur1-1} \cdot a_2 \mod n)$
$L_3$	1997/12/31	60	3	$Ur3=20$	$\sigma_3 = 0$
$L_4$	1997/12/31	40	4	$Ur4=20$	$\sigma_4 = 0$

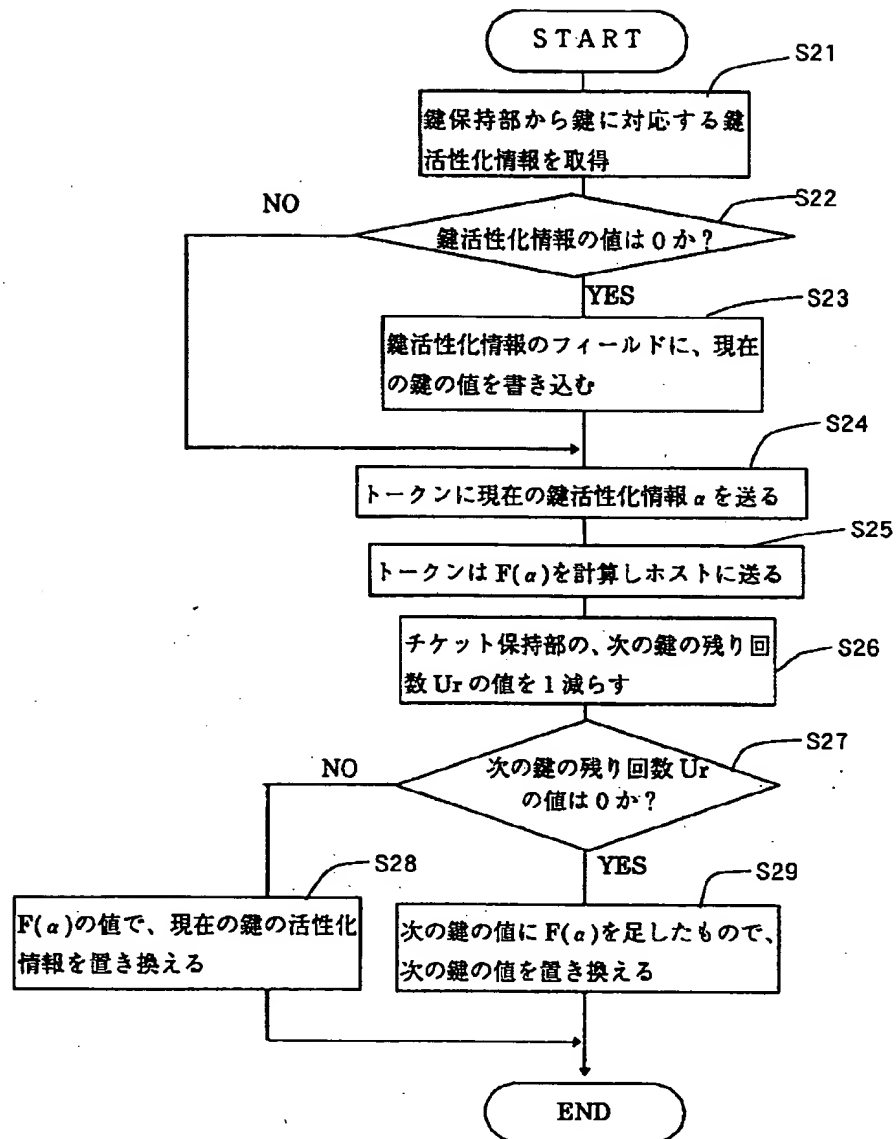
【図1】



【図2】



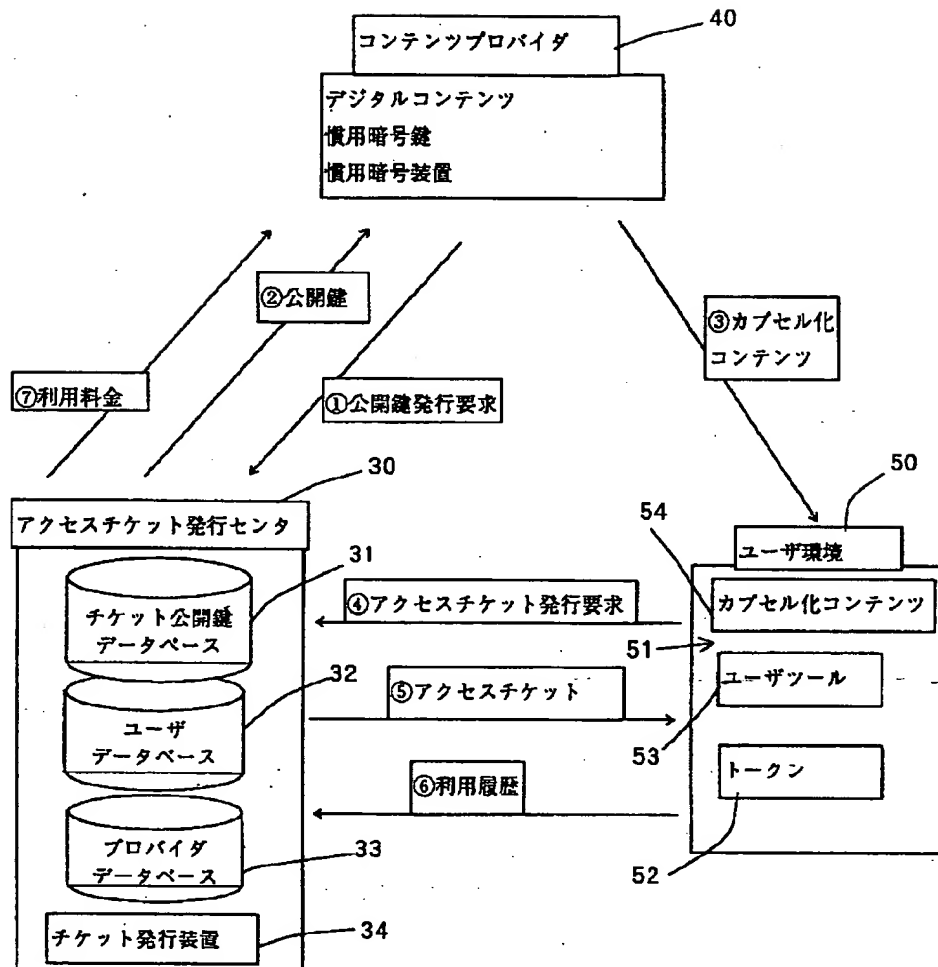
【図3】



【図19】

利用制限 情報	使用期限	利 用 料金	次のチケッ トの枚数	使用履歴を 示すフラグ f	必要な活性化 情報の数	チケット活性化情 報 $\alpha$
$L_1$	1997/12/31	100	20	0	$N_1=1$	$\alpha_1 = I_{r1}$
$L_2$	1997/12/31	100	20	0	$N_2=1$	$\alpha_2 = I_{r2}$
$L_3$	1997/12/31	100	0	0	$N_3=2$	$\alpha_3 = \alpha_1 + F(\alpha_1, \alpha_2) + \alpha_2 + F(\alpha_2, \alpha_3)$

【図6】



【図14】

利用制限情報	使用期限	利用料金	次のチケットの法数	使用可能になるまでの回数 $U_r$	チケット活性化情報 $a$
$L_1$	1997/12/31	100	$n_1$	$U_{r1}=0$	$a_1 = 1/r$
$L_2$	1997/12/31	100	$n_2$	$U_{r2}=0$	$a_2 = (a_1)^{n_1 \cdot U_{r1} + 1} \bmod n$ : $U_{r2}=20$
$L_3$	1997/12/31	100	$n_3$	$U_{r3}=0$	$a_3 = (a_2)^{n_2 \cdot U_{r2} + 1} \bmod n$ : $U_{r3}=20$
$L_4$	1997/12/31	100	0	$U_{r4}=0$	$a_4 = (a_3)^{n_3 \cdot U_{r3} + 1} \bmod n$ : $U_{r4}=20$

【図8】

利用制限情報	使用期限	利用料金	使用 順位	使用可能になる までの回数 $U_r$	チケット活性化情報 $a$
$L_1$	1997/12/31	100	1	$U_{r1}=0$	$a_1=I_r$
$L_2$	1997/12/31	80	2	$U_{r2}=0$	$a_2=(a_1)^{F_{U_{r2}}(du,L_1,n)} \bmod n$ : $U_{r2}=20$
$L_3$	1997/12/31	60	3	$U_{r3}=0$	$a_3=(a_2)^{F_{U_{r3}}(du,L_2,n)} \bmod n$ : $U_{r3}=20$
$L_4$	1997/12/31	40	4	$U_{r4}=0$	$a_4=(a_3)^{F_{U_{r4}}(du,L_3,n)} \bmod n$ : $U_{r4}=20$

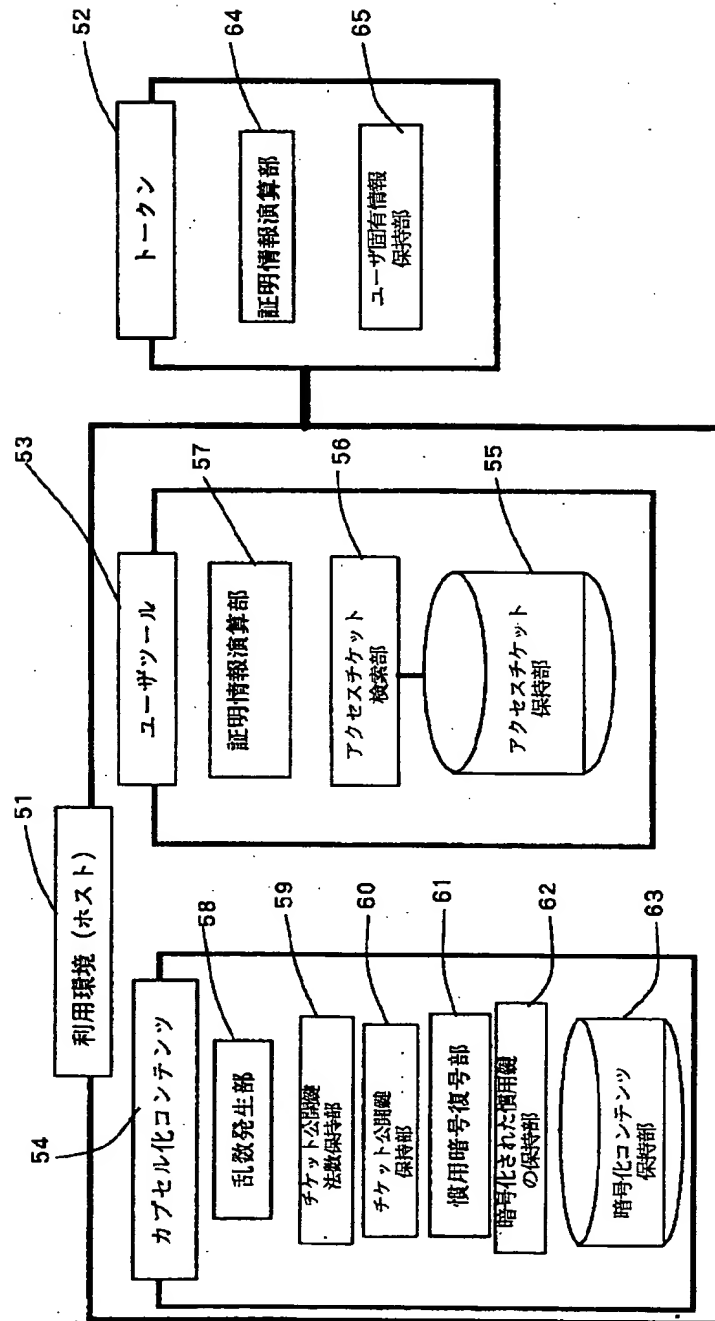
【図15】

利用制限情報	使用期限	利用料金	次のチケットの法数	使用可能になる までの回数	チケット活性化情報
$L_1$	1997/12/31	100	$m_1$	$U_{r1}=0$	$a_1=I_r$
$L_2$	1997/12/31	100	$m_2$	$U_{r2}=20$	$a_2=0$
$L_3$	1997/12/31	100	$m_3$	$U_{r3}=20$	$a_3=0$
$L_4$	1997/12/31	100	0	$U_{r4}=20$	$a_4=0$

【図20】

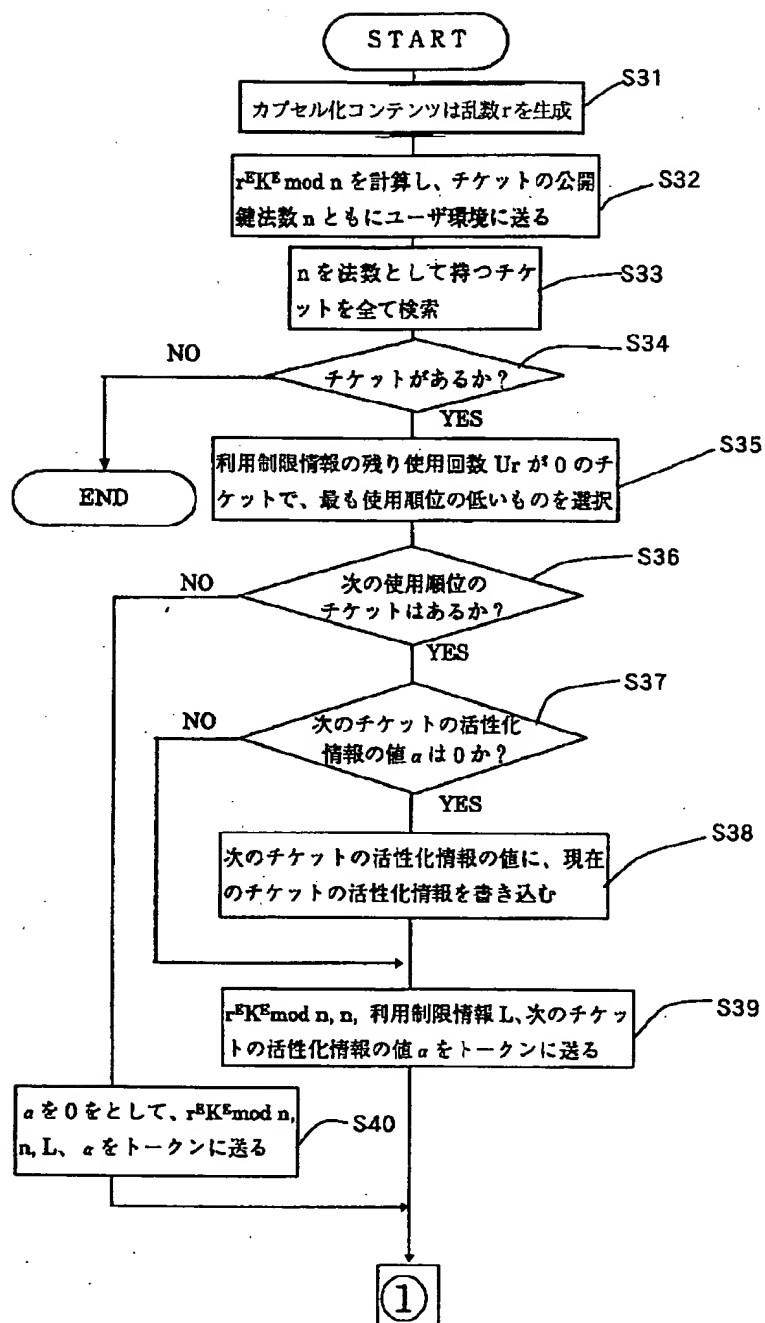
利用制限 情報	使用期限	利用 料金	次のチケットの法数	使用履歴を 示すフラグ $f$	必要な活性化 情報の数	チケット活性化情報 $a$
$L_1$	1997/12/31	100	$m_1$	0	$N_1=1$	$a_1=I_{r1}$
$L_2$	1997/12/31	100	$m_2$	0	$N_2=1$	$a_2=I_{r2}$
$L_3$	1997/12/31	100	0	0	$N_3=2$	$a_3=0$

【図10】

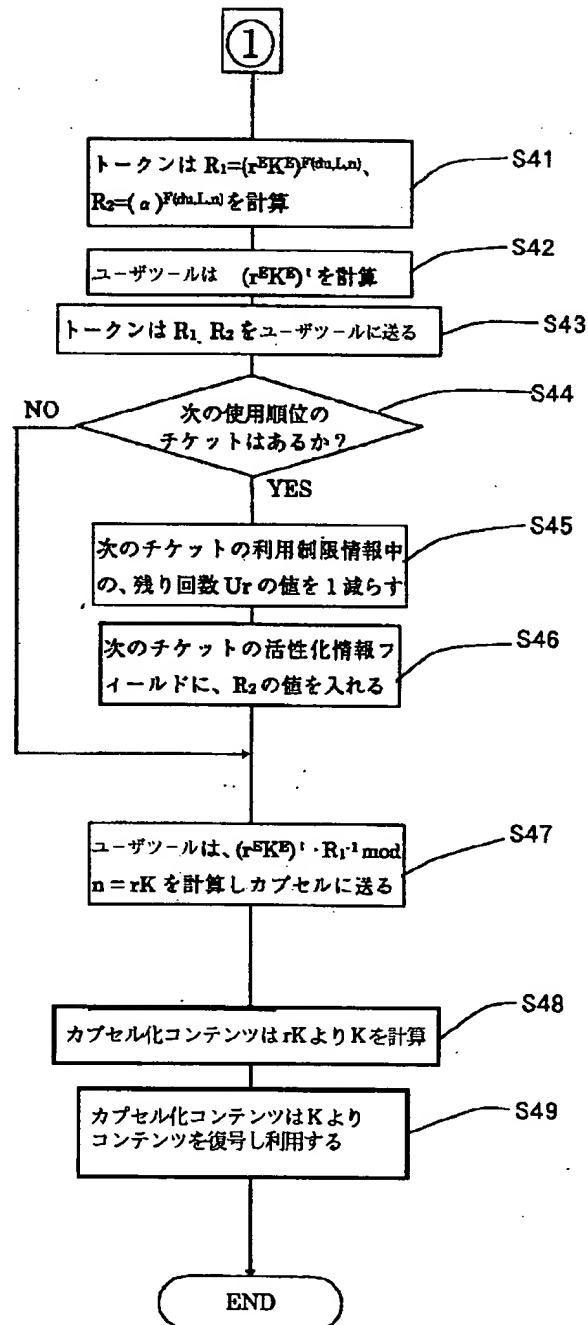




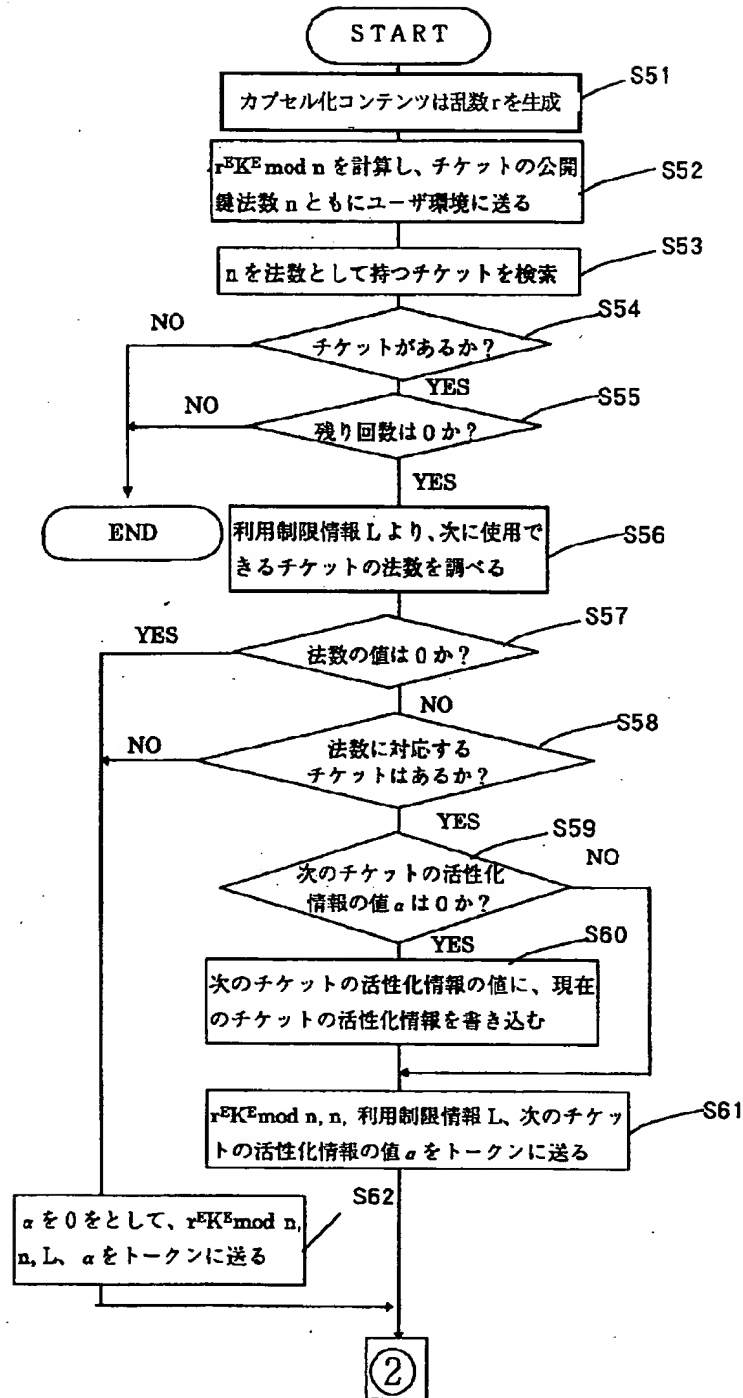
【図11】



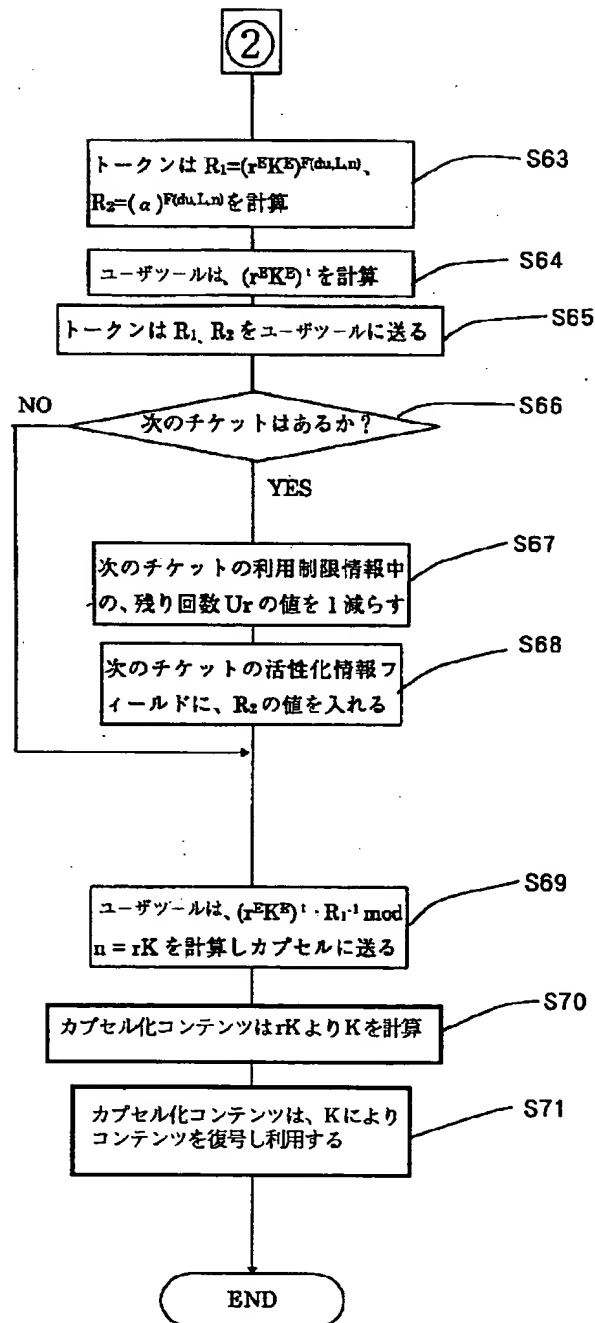
【図12】



【図16】



【図17】



【図18】

利用履歴情報	使用期限	利用料金	次のチケットの法数	使用可能になるまでの回数	チケット活性化情報
$L_1$	1997/12/31	100	$m$	$U_{r1}=0$	$a_1=1r$
$L_2$	1997/12/31	100	$m$	$U_{r2}=19$	$a_2=(a_1)^{F(m, L_1, 19)} \bmod n$
$L_3$	1997/12/31	100	$m$	$U_{r3}=20$	$a_3=0$
$L_4$	1997/12/31	100	0	$U_{r4}=20$	$a_4=0$

---

フロントページの続き

(51) Int. Cl. 6  
// G 0 6 F 12/14

識別記号  
3 2 0

F I  
H 0 4 L 9/00

6 0 1 E  
6 4 1

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-244584

(43)Date of publication of application : 19.09.1995

(51)Int.Cl.

G06F 9/06

G06F 12/14

(21)Application number : 06-032601

(71)Applicant : MATSUSHITA ELECTRIC IND CO  
LTD

(22)Date of filing : 02.03.1994

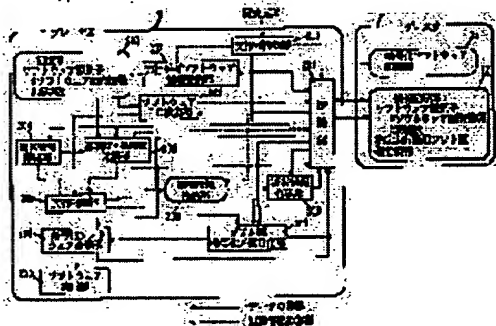
(72)Inventor : OMORI MOTOJI  
MATSUZAKI NATSUME  
TATEBAYASHI MAKOTO  
MIYAJI MITSUKO

## (54) SOFTWARE PROTECTION SYSTEM

### (57)Abstract:

**PURPOSE:** To attain execution by an optional execution device by a procedure for changing a specified execution device in a software protection system which can not be executed by an execution device other than the specified one.

**CONSTITUTION:** Whether a software identifier(ID) recorded in an information recording part 12 of a disk 1 is stored in a storage part 203 or not is retrieved. When the corresponding ID is stored in the storage part 203, the accumulated number of IDs is compared with a reference number stored in the storage part 203, and only when the accumulated number is larger, the execution of the software is permitted. Also when the corresponding ID is not stored in the storage part 203, the execution of the software is permitted. In this case, a software key in the recording part 12 is decoded by a software key ciphering/ decoding part 207, ciphered software recorded in a ciphered software recording part 11 is decoded by using the software key and executed by a software execution part 210. At the time of changing a specified execution device, the accumulated number of IDs and the reference value are changed and a software key is



rewritten to a key for a changed execution device.